



الاصطياد الإلكتروني

الأساليب والإجراءات المضادة

د. خالد بن سليمان الغثبر

م. سليمان بن عبدالعزيز بن هيشة

تقديم:

د. زياد بن عثمان الحقيل

وكيل جامعة الملك سعود للشؤون التعليمية والاكاديمية



الاصطياد الإلكتروني

الأساليب والإجراءات المضادة

تأليف

د. خالد بن سليمان الغثبر

م. سليمان عبدالعزيز الهيشة

تقديم

د. زياد بن عثمان الحقيل

وكيل جامعة الملك سعود للشؤون التعليمية والأكاديمية

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

الغثبر، خالد بن سليمان

الاصطياد الإلكتروني: الأساليب والإجراءات المضادة/

خالد سليمان عبدالله الغثبر – الرياض، 1429هـ

000 ص ؛ 17 × 24سم

ردمك: 8-1453-00-603-978

1- أمن المعلومات 2- أمن الحواسيب

أ. سليمان عبدالعزيز الهيشة (مؤلف مشارك) ب. العنوان

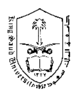
ديوي 005,8 1429/5884

رقم الإيداع: 1429/5884

ردمك: 8-1453-00-603-978

الطبعة الأولى

1429هـ - 2009م



عن المؤلّفين

* د. خالد بن سليمان الغثبر

يعمل حالياً مدير مركز التميز لأمن المعلومات بجامعة الملك سعود وعضو هيئة تدريس في كلية علوم الحاسب و المعلومات بالجامعة، و قد شارك في العديد من اللجان على مستوى الكلية و الجامعة و الوزارة، و هو مستشار لعدة جهات حكومية و خاصة. شارك في إعداد الدراسات الأمنية وتقييمها، والإشراف عليها في عدد من الجهات المختلفة. حصل على درجة البكالوريس في نظم المعلومات من جامعة الملك سعود مع مرتبة الشرف، ثم الماجستير و الدكتوراه مع مرتبة الشرف من جامعة جورج ميسن في الولايات المتحدة الأمريكية، حصل على براءة اختراع في أمن المعلومات من الولايات المتحدة الأمريكية كما حصل على شهادات تخصصية عالمية في مجال أمن المعلومات وإدارة المشاريع. له العديد من المؤلفات العلمية المتخصصة في أمن المعلومات، وكاتب في الصحف السعودية، و يقيم العديد من المحاضرات و الدورات التدريبية في مجال أمن المعلومات.

* د. سليمان عبدالعزيز الهيشة

يعمل حالياً مدير مشروع قناة التكامل الحكومية فى برنامج التعاملات الالكترونية الحكومية سابقاً خبير أنظمة التكامل في قطاع تقنية المعلومات بشركة "الاتصالات السعودية". حاصل على درجتي البكالوريوس والماجستير في نظم المعلومات من كلية علوم الحاسب والمعلومات بجامعة الملك سعود بالرياض. حاصل أيضاً على شهادة تخصصية عالمية في إدارة المشاريع (Project Management Professional) وهو باحث متعاون في مركز التميز لأمن المعلومات بجامعة الملك سعود.

الفهرس

تقديم

منذ أن بدأ عصر الإنترنت قبل قرابة عقد ونصف من الزمان واستخداماتها تتزايد بشكل مطرد، إلى أن أصبح استخدام الإنترنت أمراً لا بد منه للمؤسسات ولكثير من الأفراد. وأصبح قريباً اليوم الذي يكون فيه استخدام الإنترنت ملزماً للمؤسسات والأفراد لتنفيذ كثير من الأعمال. وكما كان توسع التجارة في القرون الماضية سبباً لتزايد القراصنة وقطاع الطرق، فإن تزايد استخدام الإنترنت أصبح سبباً لتزايد قراصنتها باختلاف أهدافهم وأساليبهم، وما يتسببون به من أخطار.

وهذا الكتاب يتناول أحد الأخطار الحديثة وهي الاصطياد الإلكتروني الذي قد يتسبب في كشف المعلومات الشخصية مثل الأرقام السرية للحسابات البنكية، وما يترتب عليها من فقدان الأموال من تلك الحسابات. ويستعرض هذا الكتاب تلك المشكلة بشكل ميسر، مبيناً أشهر أنواع الأساليب التي يتبعها المحتالون للاصطياد، وموضحاً الإجراءات السليمة للوقاية من تلك الهجمات. وقد وُفِّق المؤلفان في اختيار موضوع الكتاب لأهميته.

وإذ أنوه بالشكر للكاتبين على إثرائهما للمحتوى العربي في هذا المجال الحساس، فإنني أتمنى أن يسهم هذا الكتاب في توعية مستخدمي الإنترنت بتلك الأخطار وتقليل آثارها.

د. زياد بن عثمان الحقيل

وكيل جامعة الملك سعود للشؤون التعليمية والأكاديمية

مقدمة

أضحى البريد الإلكتروني (E-Mail) من وسائل الاتصال الحديثة والآخذة

بالانتشار المطرد مع مرور الأيام، سواء على مستوى الأفراد أو المنظمات. ففي معظم مجالات الأعمال حل البريد الإلكتروني محل الناسوخ (Fax) كأداة اتصال أساسية.

البريد الإلكتروني بصفته وسيلة تراسل مثله مثل أي وسيلة تراسل أخرى، سواء كانت إلكترونية أم لا، فإنه قد تم استغلالها بشكل سيىء عن طريق استخدامها لأهداف غير الأهداف الأساسية التي بُني عليها نظام البريد الإلكتروني.

يناقش هذا الكتاب مختلف الأساليب المستخدمة في استغلال البريد الإلكتروني بشكل سيىء، والإجراءات المضادة لها؛ وقد تم تقسيم الكتاب إلى خمسة فصول. الفصل الأول يشرح نظام البريد الإلكتروني، والفصل الثاني يناقش رسائل البريد الإلكتروني غير المرغوبة (Spam)، ويُعَد مقدمة لموضوع الكتاب الرئيس وهو الاصطياد الإلكتروني (Phishing) والذي سيكون موضوع الفصول من الثالث إلى الخامس.

تبدو أهمية هذا الكتاب في كونه مادة توعوية باللغة العربية موجهة لمستخدمي الحاسب والشبكة العالمية (Internet) الذين يمثل التراسل عبر البريد الإلكتروني أحد أنشطتهم اليومية في ظل النقص الحاد للمحتوى العربي في مجال مهم وحساس كمجال أمن المعلومات.

الفصل الأول
نظام البريد الإلكتروني

- مكونات نظام البريد الإلكتروني
- البريد الإلكتروني المعتمد على الشبكة العالمية
- برتوكولات تراسل البريد الإلكتروني
- استخدام نظام أسماء النطاقات في نظام البريد الإلكتروني
- هيكلية رسالة البريد الإلكتروني

يشرح هذا الفصل ماهية نظام البريد الإلكتروني من حيث مكوناته، وطريقة عملها بعضها مع بعض. ويشرح أيضاً كيفية تراسل البريد الإلكتروني عبر الشبكة العالمية من حيث البرتوكولات المُستخدمَة في التراسل، ودور نظام أسماء النطاقات في عملية تراسل البريد الإلكتروني. وفي آخر هذا الفصل شرح لهيكلية رسالة البريد الإلكتروني.

1.1 مكونات نظام البريد الإلكتروني

تتكون التطبيقات (Applications) المبنية على شبكة البيانات (Data Network) من عميل (client)، وخادم (server). وبما أن البريد الإلكتروني تطبيق مبني على شبكة البيانات فهو يتكون من عميل البريد الإلكتروني (E-Mail Client) وخادم البريد الإلكتروني (E-Mail Server).

1.1.1 عميل البريد الإلكتروني (E-Mail Client)

يسمى أيضاً وكيل بريد المستخدم (Mail User Agent-MUA)، وهو الواجهه البينية بين المستخدم، وخادم البريد الإلكتروني (E-Mail Server).

وظائف عميل البريد الإلكتروني هي:

- استرجاع البريد من حساب البريد في الخادم (E-Mail Server) باستخدام بروتوكول مكتب البريد (POP3).
- ضبط الرسائل استناداً إلى القياسات المعتمدة للإرسال.
- تسليم الرسائل إلى الخادم (E-Mail Server) باستخدام برتوكول نقل البريد البسيط (SMTP).

يوضح الشكل (1-1) موقع عميل البريد الإلكتروني في نظام البريد الإلكتروني.

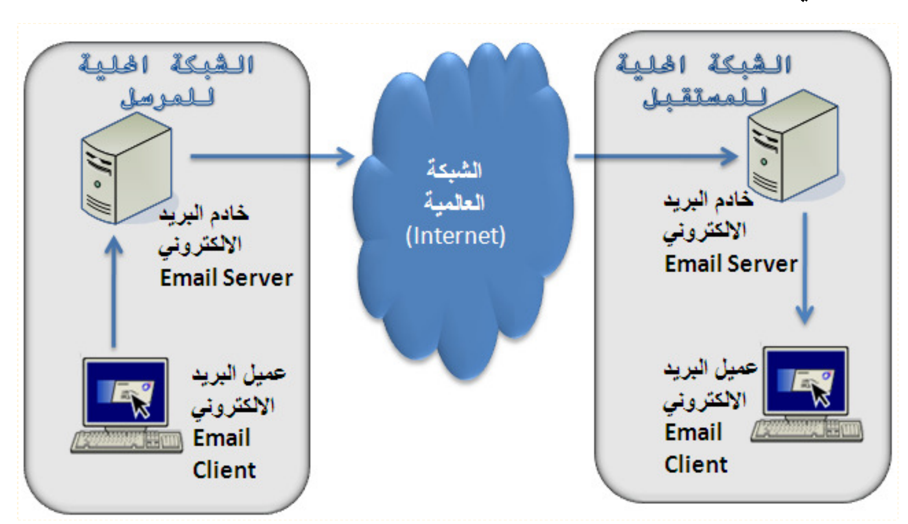
من الأمثلة على برامج عميل البريد الإلكتروني برنامج "Microsoft Outlook"(1) من شركة "مايكروسوفت".

2.1.1 خادم البريد الإلكتروني (E-Mail Server)

ويسمى أيضاً وكيل نقل البريد (Mail Transfer Agent–MTA). وهو الذي يقوم بعملية استقبال و ارسال البريد الإلكتروني من و إلى خوادم البريد الإلكتروني الأخرى على الشبكة العالمية (Internet).

من الأمثلة على برامج خوادم البريد الإلكتروني برنامج "Microsoft Exchange Server"(2) من شركة "مايكروسوفت".

يوضح أيضاً الشكل (1 -1) موقع خادم البريد الإلكتروني في نظام البريد الإلكتروني.



اشكل (1–1) نظام البريد الإلكتروني

(1) موقع البرنامج على الشبكة العالمية (www.microsoft.com/outlook/)

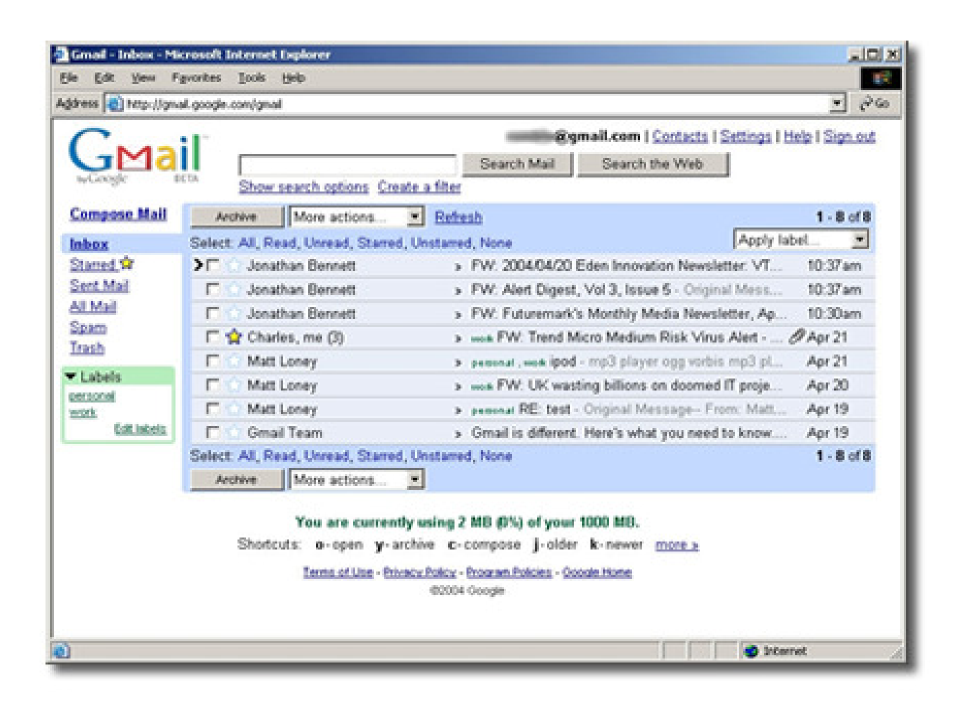
(2) موقع البرنامج على الشبكة العالمية (www.microsoft.com/exchange/default.mspx)

2.1 البريد الإلكتروني المبني على الشبكة العالمية

(Web-based E-Mail – webmail)

هي خدمة بريد إلكتروني معدة للاتصال من خلال متصفح الشبكة العالمية (Internet)، يُمثِل فيها متصفح الشبكة العالمية دور عميل البريد الإلكتروني.

من الأمثلة على البريد الإلكتروني المعتمد على الشبكة العالمية خدمة "Gmail" (gmail.com) من شركة "جوجل" (google.com)؛ كما هو موضح في الشكل (2-1).



شكل 1-2 البريد الإلكتروني المبني على الشبكة العالمية

3.1 بروتوكولات تراسل البريد الإلكتروني

لتراسل البريد في نظام البريد الإلكتروني، يلزم وجود بروتوكلات قياسية مُعتمِدة، يتسنى لكل طرف في عملية تراسل، سواء بين العميل والخادم أو فيما بين الخوادم من خلالها اتباع خطوات محددة تُمكِّن من استقبال البريد الإلكتروني وإرساله.

1.3.1 بروتوكول نقل البريد البسيط

(Simple Mail Transfer Protocol - SMTP)

هو البروتوكول القياسي المُعتمَد لتراسل البريد الإلكتروني على الشبكة العالمية، وتم تعريفه بوثيقة طلب التعليقات (RFC) رقم 821 [1] والوثيقة الملحقة رقم 1123 [2].

تستقبل خوادم البريد الإلكتروني اتصالات بروتوكول نقل البريد البسيط على المنفذ رقم 25 (Port 25)، كما هو موضح في الشكل (1-3). ومن الممكن تغيير رقم المنفذ من قبل مدير الخادم.

2.3.1 برتوكول مكتب البريد

(POP3 – Post Office Protocol)

هو البرتوكول الذي يستخدمه عميل البريد الإلكتروني لاسترجاع البريد الإلكتروني من الخادم. تم تعريف هذا البرتوكول بوثيقة طلب التعليقات رقم

---

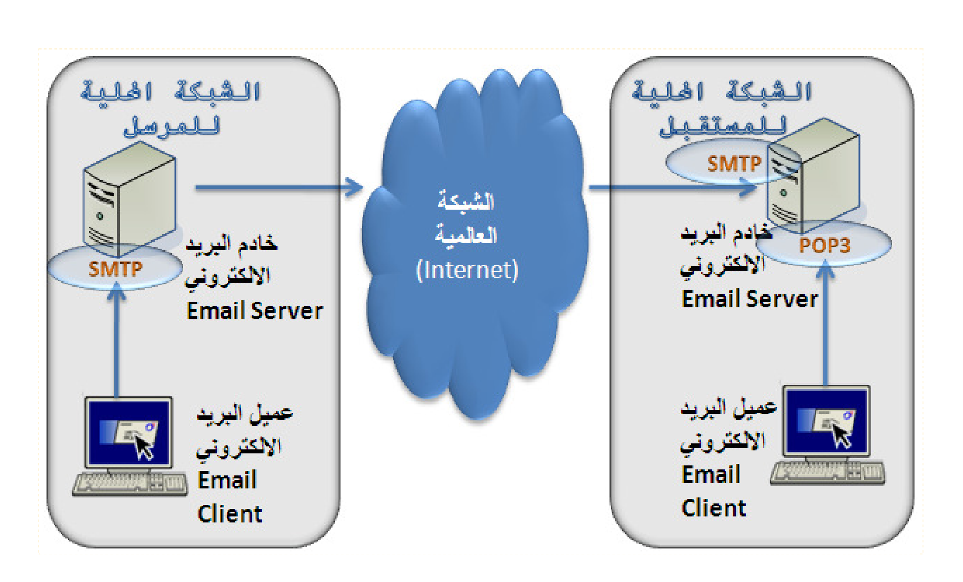
(1) النسخة الإلكترونية من الوثيقة (http://tools.ietf.org/html/rfc821) .

(2) النسخة الإلكترونية من الوثيقة (http://tools.ietf.org/html/rfc1123) .

1939 .1

علماً بأن الرقم 3 من اسم البرتوكول يشير إلى النسخة الحالية المستخدمة من هذا البرتوكول، وهي النسخة الثالثة.

تستقبل خوادم البريد الإلكتروني اتصالات بروتوكول مكتب البريد على المنفذ رقم 110(Port 110)، كما هو موضح في الشكل (1-3). ويمكن أن يغير مدير الخادم رقم المنفذ.



شكل (1-3) منافذ SMTP و POP3

4.1 استخدام نظام أسماء النطاقات في نظام البريد الإلكتروني

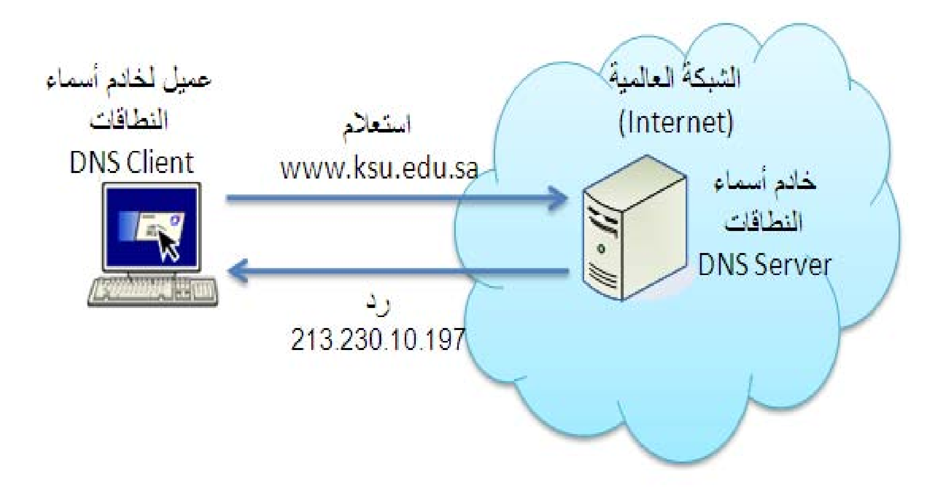
اسم النطاق هو الجزء الذي يأتي بعد علامة "@" في عنوان البريد الإلكتروني.

---

(3) النسخة الإلكترونية من الوثيقة (http://tools.ietf.org/html/rfc1939) .

فمثلاً اسم النطاق للعنوان البريدي "xyz@abc.com" هو "abc.com".

نظام أسماء النطاقات (Domain Name System - DNS) هو أحد المكونات الأساسية للشبكة العالمية، ويتكون من عدة خوادم تعمل بشكل متكامل فيما بينها. أهم خدمات هذا النظام هو الربط بين أسماء النطاقات وعناوينها العشرية، حيث لابد من معرفة العنوان العشري للخادم المراد التخاطب معه، أي إنه يمكن اعتباره دليل الهاتف بالنسبة للشبكة العالمية. فعلى سبيل المثال عنوان جامعة الملك سعود (www.ksu.edu.sa) العنوان العشري المسجل لها (213.230.10.197)، وبيانات الربط هذه تكون موجودة ومتاحة للاستعلام في أحد خوادم أسماء النطاقات، كما هو موضح في الشكل (1-4).



شكل (1-4) الاستعلام من خادم أسماء النطاقات

إحدى الخدمات الأخرى التي يقدمها نظام أسماء النطاقات هي الاستعلام عن أسماء خوادم البريد الإلكتروني المرتبطة باسم نطاق معين. فقد يكون هناك أكثر

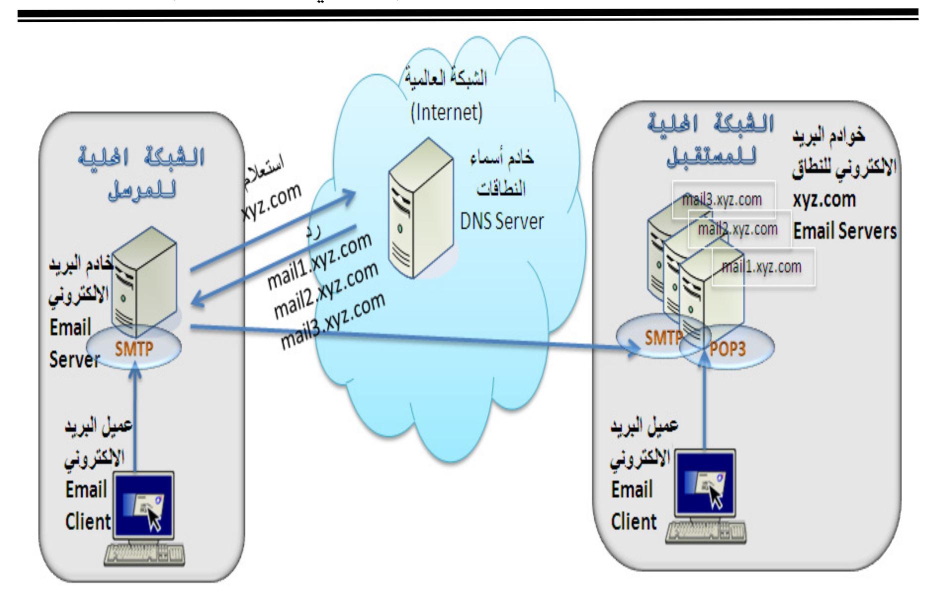
من خادم بريد إلكتروني لإسم نطاق واحد، ويعود السبب وراء ذلك إما لتوفير خوادم مساعدة لغرض توزيع حمل الطلبات الكثيرة على اسم النطاق بين الخوادم (Load Balancing)، أو لتوفير خوادم احتياطية (Backup ، أو Failover).

في حالة الاستعلام بالنسبة لخوادم البريد الإلكتروني، فإن خادم أسماء النطاقات يرد بسجلات تعرف بـ "سجلات تبادل الرسائل" (Mail exchange Records – MX records).

5.1 سجلات تبادل الرسائل

(Mail exchange records – MX records)

تحدد سجلات تبادل الرسائل كيفية إيصال الرسالة، وذلك بتزويد المُستَعلِم بأسماء خوادم البريد الإلكتروني للمُستقبِل مع رقم تفضيلي لكل خادم (preference number).



شكل (1–5) سجلات تبادل الرسائل

الغرض من الرقم التفضيلي هو ترتيب الخوادم. فكلما كان رقم التفضيل أصغر كانت احتمالية النجاح أكبر في توصيل الرسالة، ولهذا فإن الخادم المُرسِل يحاول الاتصال أولاً مع الخادم ذي الرقم الأدنى، فإن لم ينجح الاتصال معه لسبب ما فإنه يحاول مع الخادم الذي يليه، كما هو موضح في الشكل (1–5).

6.1 هيكلية رسالة البريد الإلكتروني

يتكون البريد الإلكتروني من عدة أجزاء، هي:

- **ترويسة رأس الرسالة (Header)**

وتحتوي على البيانات التالية

- المُرسِل (From): يمثل العنوان البريدي للمُرسِل، ويكون على الصيغة: [sender]@[source domain name].

sender : اسم حساب البريد الإلكتروني للمُرسِل

source domain name : اسم النطاق للخادم الذي صدرت منه الرسالة.

- المُستقبِل (To): يمثل العنوان البريدي للمُستقبِل. ويمكن أن يحوي عنواناً مُستقبِلاً وحيداً، أو مجموعة مُستقبِلين. يكون عنوان المُستقبِل على الصيغة [receiver]@ [destination domain name] .

receiver : اسم حساب البريد الإلكتروني للمُستقبِل

destination domain name : اسم النطاق للخادم الذي ستُورَد الرسالة إليه.

- المسار (Route) : بيان تفصيلي لمسار الرسالة من خادم البريد الإلكتروني المُرسِل إلى خادم البريد الإلكتروني المُستقبِل، مروراً بالخوادم الوسيطة الأخرى، مرتبة حسب التسلسل الزمني من الأسفل إلى الأعلى. عادة لاتعرض برامج عميل البريد الإلكتروني بيانات المسار مباشرةً مع البريد ، لكن بإمكان المُستخدِم عرضها عن طريق خيارات متوفرة في برامج عميل البريد الإلكتروني، كخيار "إظهار الأصلية" في عميل البريد الإلكتروني "جوجل". والشكل (1-7) يعرض مثالاً للمسار.

- **الموضوع (Subject)**: يمثل موضوع الرسالة.
- **النَص (Body)**: يمثل نص الرسالة.

شكل (1-6) رسالة بريد إلكتروني

من: xyz@a-company.com
إلى: abc@b-company.com
الموضوع: مثال لرسالة البريد الإلكتروني

هذا مثال لرسالة البريد الإلكتروني

شكل (1–7) مسار رسالة بريد إلكتروني

```
Delivered-To: abc@b-company.com
Received: by 10.141.45.1 with SMTP id x1cs19411rvj;
        Thu, 17 Jan 2008 14:35:34 -0800 (PST) ←خادم المستقبل
Received: by 10.100.44.4 with SMTP id
r4mr5496105anr.55.1200609333232;
        Thu, 17 Jan 2008 14:35:33 -0800 (PST) ←الخادم الوسيط الثاني
Received: by 10.100.167.15 with HTTP; Thu, 17 Jan 2008
14:35:06 -0800 (PST) ←الخادم الوسيط الأول
```

الفصل الثاني
رسائل البريد الإلكتروني غير المرغوبة
(Spam)

- مقدمة عن رسائل البريد الإلكتروني غير المرغوبة
- أساليب رسائل البريد الإلكتروني غير المرغوبة
- الإجراءات المضادة لرسائل البريد الإلكتروني غير المرغوبة

يناقش هذا الفصل رسائل البريد الإلكتروني غير المرغوبة من حيث تعريفها وأهدافها، وما تسببه من أضرار على مستوى الأفراد والمنظمات.

وبعد ذلك يناقش هذا الفصل الأساليب المستخدمة في إرسال البريد الإلكتروني غير المرغوب، والإجراءات المضادة لها.

1.2 مقدمة عن رسائل البريد الإلكتروني غير المرغوبة (Spam)

تعرف رسائل البريد الإلكتروني غير المرغوبة بأنها إساءة استخدام نظام الرسائل الإلكترونية (Electronic Messaging System) بإرسال كم هائل (Bulk) من الرسائل العشوائية وغير المطلوبة أو المتوقعة أو المرغوبة من قبل المُستقبلين لهذه الرسائل. ولقد شاع ارتباط كلمة (Spam) بنظام البريد الإلكتروني (Electronic Mail)، أو اختصاراً (E-Mail)، إلا إنها تنطبق أيضاً على أي وسيط للرسائل الإلكترونية مثل:

- المدونات (Blogs).
- الرسائل النصية القصيرة (SMS).
- المنتديات (Forums).
- محركات البحث (Web Search Engines).
- التراسل الآني / التراسل المباشر (Instant Messaging).

غالباً ما يكون الغرض من هذه الرسائل هو الإعلان التجاري، ومن خلالها يلجأ المعلنون للإعلان عما يريدون بيُسر وتكلفة زهيدة، نظراً لانعدام التكاليف التشغيلية المرتبطة عادة بهذه الإعلانات. فما على المُعلِن سوى تجهيز المادة الإعلانية

ونشرها عبر أي نظام رسائل بتكلفة ضئيلة مقارنةً بوسائل الإعلان الأخرى.

هناك أيضاً أغراض أخرى تُستغَل فيها هذه الرسائل كالاحتيال، وهذه تدخل تحت باب الهندسة الاجتماعية (Social Engineering) حيث لاتتضمن هذه الطريقة استغلالاً للثغرات التقنية بقدر ماتستغل الجانب الاجتماعي البشري عند مُستقبل الرسالة. مثالاً على هذا النوع رسائل "الاستثمارات البترولية في نيجيريا" التي كان الهدف منها إقناع مُستقبل الرسالة بتحويل مبالغ مالية من أجل استثمارات هي في الحقيقة وهمية. ومثالاً آخر هو محاولة إقناع مُستقبل الرسالة بفتح ملف مرفق مع الرسالة بإيهامه بأن هذا الملف ملف نصي، أو صورة، أو مقطع فيديو، بينما في الحقيقية هو فيروس..!

في إحصائية 1 أصدرها البرنامج الوطني السعودي لمكافحة الرسائل الاقتحامية (غير المرغوبة) (National Saudi Anti-Spam Program)، تبين أن نسبة البريد الإلكتروني غير المرغوب بناءاً على المعلومات التي تم جمعها من مزودي خدمة الشبكة العالمية (ISP) بلغت 54٪ لعام 2007م، وكان معظمها رسائل تسويقية. وأظهرت الإحصائية أيضاً أن نسبة الرسائل النصية القصيرة غير المرغوبة (SMS Spam) بناءاً على المعلومات الواردة من مشغلي الهاتف النقّال في السعودية - بلغت 1.7٪ لعام 2007م، 65٪ منها تجارية، 20٪ بذيئة، 2٪ سياسية، 3٪ دينية، 5٪ تتعلق بأسواق الأسهم، و5٪ ذات أغراض أخرى.

(1) "تقييم الوضع الراهن للرسائل الاقتحامية في المملكة العربية السعودية"، هيئة الاتصالات وتقنية المعلومات، 1429هـ- 2008م، (http://www.spam.gov.sa/Statistics-Arabic.doc)

أظهر تقرير شهري [1] أصدرته شركة: "سيمانتك" (Symantec) [2] عن رسائل البريد الإلكتروني غير المرغوبة لشهر فبراير من عام 2007 أن نسبة البريد الإلكتروني غير المرغوب يمثل 69٪ من إجمالي رسائل البريد الإلكتروني. وفي تقرير [3] آخر أصدرته شركة "كوم تتش" (Commtouch) [4] أظهر أن هذه النسبة لعام 2005 بلغت 67٪ وفي عام 2006 بلغت 87٪ أي 140 مليار رسالة من إجمالي 160 مليار رسالة، بزيادة قدرها 30٪ عن عام 2005.

تشكل هذه النسبة العالية مصدر إزعاج للأفراد والمنظمات. فبالنسبة للمنظمات هناك أخطار مالية وأمنية يمكن أن تُحدِثها هذه الرسائل. فعلى الجانب المالي:

- ساعات العمل الضائعة لقراءة هذا الرسائل وتصفيتها من قبل الموظفين.
- المساحة التخزينية الضائعة لحفظ هذا الرسائل لحين قراءتها من قبل المُستقبل (الموظف).
- التدفق (Traffic) غير الضروري على خادم البريد الإلكتروني (E-Mail Server) للمنظمة.
- الاستهلاك غير الضروري لسعة قناة الاتصال (Data Network

(1) The State of Spam, A Monthly Report – February 2007, Generated by Symantec Messaging and Web Security (http://www.symantec.com/avcenter/reference/Symantec_Spam_Report_-_February_2007.pdf)

(2) هي شركة متخصصة في مجال تطبيقات أمن المعلومات (Symantec.com)

(3) 2006 Spam Trends Report: Year of the Zombies, December 27, 2006, Commtouch® Software Ltd., (http://www.commtouch.com/documents/Commtouch_2006_Spam_Trends_Year_of_the_Zombies.pdf)

(4) هي شركة متخصصة في برمجيات أمن المعلومات للبريد الإلكتروني (http://www.commtouch.com)

Bandwidth) للمنظمة، وأيضاً لسعة الاتصال عبر الشبكة العالمية (Internet). وقد أظهر تقرير الرسائل غير المرغوبة [1] لعام 2006، الصادر عن شركة "كوم تتش" (Commtouch) [2] أن هذه الرسائل استهلكت 1700 تيرا [3] بايت [4] (1,700,000,000 ميكا [5] بايت) في عام 2006 وأن استخدام الصور (Images) في هذه الرسائل قد رفع نسبة الاستهلاك لما تتطلبه الصور من عدد كبير من البايتات (Bytes) لحفظها وتمثيلها، مقارنة بالنصوص (Text).

في دراسة [6] أجرتها الهيئة التشريعية بولاية كاليفورنيا بالولايات المتحدة الأمريكية أظهرت أن هذه النوعية من الرسائل كلفت المنظمات الأمريكية وحدها أكثر من 13 ملياراً في عام 2007، وتشمل هذه التكلفة الإنتاجية الضائعة وتكاليف المعدات والبرمجيات، والقوى العاملة اللازمة للتصدي لهذه الرسائل.

وعلى الجانب الأمني:

- يمكن لهذه الرسائل أن تعرض جهاز المُستقبل، وأيضاً الشبكة التي يعمل عليها هذا الجهاز لمشاكل هجمات الفيروسات عن طريق الملفات المرفقة مع الرسالة

---

(1) 2006 Spam Trends Report: Year of the Zombies, December 27, 2006, Commtouch® Software Ltd., (http://www.commtouch.com/documents/Commtouch_2006_Spam_Trends_Year_of_the_Zombies.pdf)

(2) هي شركة متخصصة في برمجيات أمن المعلومات للبريد الإلكتروني (http://www.commtouch.com).

(3) بادئة تعني 1000 بليون.

(4) بايت (byte) هي وحدة قياس تخزين المعلومات في الحاسوب وتتكون من 8 بت (bit). الـ"بت" له قيمتان إما "1" أو "0".

(5) بادئة تعني 1 مليون.

(6) دستور كاليفورنيا للأعمال والتخصصات (http://www.spamlaws.com/state/ca.shtml).

الإلكترونية، أو عن طريق روابط الشبكة العالمية المضمنة بالرسالة، والتي قد تؤدي بدورها إلى تنفيذ ملف فيروس أو تحميله. ومثالاً على هذه الطريقة دودة "MyDoom"، التي اكتشفت في يناير 2004. انتشرت هذه الدودة عن طريق فتح الملف المرفق مع رسالة بريد إلكتروني، وذلك بإيهام المُستقبِل الرسالة بأن الملف المرفق ملف نصي مشفر وفي الحقيقة هو دودة "MyDoom"، وعند فتح المستقبل لهذا الملف المرفق فإن جهازه يصبح مصاباً بهذه الدودة، فيقوم من أثر الإصابة بإرسال نسخة من الرسالة إلى عناوين بريد إلكترونية أخرى محفوظة في جهاز الضحية [1].

●جرائم يتم استخدام الرسائل غير المرغوبة فيها من أجل التغرير بالناس لأهداف مختلفة، وهي رسائل الاحتيال كرسالة "الاستثمارات البترولية في نيجيريا" السابق ذكرها. ومن الأمثلة أيضاً مقتل الثري اليوناني في جمهورية جنوب أفريقيا. تبدأ هذه القصة عندما أرسل المجرمون رسالة لكم هائل من العناوين البريدية تَعِدْ بجني مئات الآلاف من الراند [2]، وكان من المُستقبِلين العشوائيين لهذا البريد هو أحد الأثرياء اليونايين، والذي انطلت عليه الكذبة ونفذ المطلوب منه بالبريد، وهو أن يذهب إلى عنوان محدد بأحد أرياف جمهورية جنوب أفريقيا، وعند وصوله قام المجرمون باختطافه وطالبوا بفدية من أهله لإطلاق سراحه، ولما لم يستلموا الفدية قتلوه، فكان ضحيه، لهذا البريد غير المرغوب [3].

---

(1) خدمة وصف الفيروسات من شركة أمن المعلومات "F-Secure" (http://www.f-secure.com/v-descs/novarg.shtml).

(2) الراند (Rand) هي العملة النقدية لجمهورية جنوب أفريقيا.

(3) جريدة "أخبار 24" الجنوب أفريقية بتاريخ 31\ديسيمبر\2004 بعنوان "SA cops, Interpol probe murder" (http://www.news24.com/News24/South_Africa/News/0,,2-7-1442_1641875,00.html).

2.2 أساليب الرسائل البريدية الإلكترونية غير المرغوبة

يناقش هذا الجزء مختلف الأساليب المستخدمة في إرسال رسائل البريد الإلكتروني غير المرغوبة.

1.2.2 الأسلوب الأول: بريد انتحال الشخصية (E-Mail Spoofing)

يفتقد برتوكول نقل البريد البسيط (SMTP) إلى خاصية التصديق (Authentication) على المُرسِل، أى إنه بالإمكان إرسال رسالة بأي عنوان بريد إلكتروني عن طريق التلاعب بترويسة رأس الرسالة (Header)، وتحديدا بالحقل "من" (From) الذي يمثل عنوان المُرسِل. فالرسالة القادمة من عنوان بريد إلكتروني لاتعكس بالضرورة حقيقة شخصية المُرسِل. وهذا الجانب تم استغلاله في إرسال البريد غير المرغوب عن طريق الاحتيال (spoofing)، ويعمد مُرسِلو هذه الرسائل إلى اختيار عناوين براقة وشائعة كاسم مصرف أو شركة معروفة، وذلك لأجل إيهام المُستقبِل بجدية الرسالة وأنها قادمة من مصدر موثوق.

وللاحتياط من هذا النوع من الرسائل ينصح بعدم فتح الملفات المرفقة (Attachments)، أو الروابط (Links) الموجودة في الرسالة إذا لم تكن الرسالة متوقعة. فالملفات المرفقة قد تكون فيروسات، والروابط قد تؤدي إلى تحميل فيروسات، أو تنقل إلى مواقع مصابة.

2.2.2 الأسلوب الثاني: خادم البريد الإلكتروني المفتوح (Open Mail Rely)

بعض خوادم البريد الإلكتروني تقبل رسائل البريد الإلكتروني من أي مصدر كان لتمريرها إلى خوادم أخرى، وهذه الطريقة كانت مهمة في الأيام الأولى للشبكة

العالمية لضمان إيصال رسالة البريد الإلكتروني نظراً لقلة اعتمادية الشبكة العالمية تلك الأيام، فإذا كان الخادم الذي صدرت منه الرسالة غير قادر على الاتصال بخادم المُستقبِل فإنه على الأقل بإمكانه إيصالها إلى خادم آخر مفتوح قريب من خادم المُستقبِل، فيكون هناك فرصة أفضل للخادم المفتوح في إيصال الرسالة في وقت آخر. هذه الآلية في التراسل شكلت ثغرة أمنية تم استغلالها من قبل مُرسِلي الرسائل غير المرغوبة؛ ونظراً لذلك فإن عدداً قليلاً من الخوادم الحديثة تكون خوادم مفتوحة والعديد من الخوادم الحديثة لايقبل الرسائل القادمة من الخوادم المفتوحة لأن هناك احتمالاً قوياً بأن تكون هذه الرسائل غير مرغوبة.

3.2.2 الأسلوب الثالث: الرسائل غير المرغوبة المعتمدة على الصور

(Image-based Spam)

يلجأ مُرسِلو الرسائل غير المرغوبة إلى استخدام الصور في نص الرسالة لتفادي عملية التصفية المعتمدة على المحتوى النصي، وفيها يتم تضمين النص على هيئة صورة في نَص الرسالة.

أظهر تقرير الرسائل غير المرغوبة [1] لعام 2006 أصدرته شركة: "كوم تتش" (Commtouch) [2] أن نسبة الرسائل غير المرغوبة، المعتمدة على الصور مثلت 35٪ من إجمالي عدد الرسائل غير المرغوبة وأنها استهلكت 70٪ من إجمالي سعة قناة تدفق البيانات (Data Traffic Bandwidth) المستهلك من الرسائل غير المرغوبة

(1) 2006 Spam Trends Report: Year of the Zombies, December 27, 2006, Commtouch® Software Ltd., (http://www.commtouch.com/documents/Commtouch_2006_Spam_Trends_Year_of_the_Zombies.pdf)

(2) هي شركة متخصصة في برمجيات أمن المعلومات للبريد الإلكتروني (http://www.commtouch.com)

المقدرة بـ: 1700 تيرا بايت (1,700,000,000 ميجابايت).

وقد تبين أن استخدام الصور في هذه الرسائل رفع نسبة استهلاك سعة نطاق تدفق البيانات لما تتطلبه الصور من عدد كبير من البايتات (Bytes) لحفظها وتمثيلها، مقارنة بالنصوص (Text).

قد يساعد التعرف على الحروف ضوئيا (Optical Character Recognition – OCR) والطرق التجريبية (heuristic methods) للتعرف على المظاهر (patterns) المستخدمة في تصفية الرسائل بشكل محدود في التصدي لمثل هذا النوع من الرسائل غير المرغوبة، كون معظمها أخذ أشكالاً معقدة في تمثيل النصوص على هيئة صور. فعلى سبيل المثال:

- تغيير اللون وشكل النص والحجم لكل رسالة.
- فصل الحروف.
- وضع بقع ملونة على الصورة بلون مختلف لكل رسالة مرسلة.
- استخدام الصور المتحركة.

التصفية وحدها ليست كافية للتصدي للرسائل غير المرغوبة، فاستخدام أكبر قدر ممكن من الإجراءات المضادة للرسائل غير المرغوبة، سيعطي نتيجة فعالة في التقليل من الرسائل غير المرغوبة إلى أقل قدر ممكن.

لايتوقف مُرسِلي الرسائل غير المرغوبة عند مزج النص بالصور فقط، بل يتعدى إلى استخدام صيغ هيئات ملفات أخرى، كتضمين النص في ملفات الوثائق المحمولة (PDF)، أو إلى صيغ ملفات برامج المكتب من "مايكروسوفت" (Microsoft Office) مثل (DOC) و (XLS).

4.2.2 الأسلوب الرابع: هجمة القاموس (Dictionary Attack)

قد يستخدم مُرسِلو البريد غير المرغوب القاموس في تخمين عناوين بريد إلكترونية، وذلك عن طريق إضافة أسماء ذات معنى لأسماء نطاقات مشهورة؛ وبهذه الطريقة يشكلون عناوين بريد إلكترونية.

الأسماء المنتجة عادة ما تكون من قاموس لأسماء و ألقاب مشهورة. وحتى إن كانت معظم الأسماء المنتجة غير موجودة في الواقع إلا أن المجهود يستحق البذل في تخمين ولو عدد قليل من العناوين الصحيحة بالنظر إلى بساطة الطريقة في إيجاد هذه العناوين.

وبالإمكان التعرف على العناوين النشيطة من مجموعة العناوين المنتجة من القاموس، كون الرد على الرسالة، أو تتبع الرابط المضمن في نَص الرسالة يعطي دلالة للمُرسِل على أن بريد المُستقبِل نشيط، ما يجعل المُرسِل يستخدمه عند إرسال المزيد من الرسائل غير مرغوبة.

3.2 الإجراءات المضادة لرسائل البريد الإلكتروني غير المرغوبة

يناقش هذا الجزء مختلف الإجراءات المضادة لرسائل البريد الإلكتروني غير المرغوبة.

1.3.2 الإجراء المضاد الأول: التصفية (Filtration)

تكون تصفية الرسائل البريد الإلكتروني على أساس أحد أجزاء الرسالة التالية:

- أحد مكونات ترويسة رأس الرسالة (Header)، ومنها عنوان المُرسِل (From).

- موضوع الرسالة (Subject) .
- نَص الرسالة (Body) .

فإذا تطابقت إحدى خصائص البريد القادم مع إحدى القيم المُعرَّفَة لعملية التصفية على أنها كعناوين بريد إلكترونية، أو قيم محددة بالنسبة لترويسة رأس الرسالة أو تعبيرات مألوفة (regular expressions) بالنسبة للموضوع أو النَص فإن الخادم يتخذ قراراً بشأن هذا البريد الوارد.

التصفية هي أكثر الإجراءات المطبقة للتصدي للرسائل غير المرغوبة، لكنها عرضة للعديد من التجاوزات للقوانين المعتمدة عليها عملية التصفية، خاصة من مرسلي الرسائل غير المرغوبة الذين عادة مايكونون دقيقين وخبيرين في قوانين التصفية [1].

2.3.2 الإجراء المضاد الثاني: القوائم البيضاء والقوائم السوداء (Black lists / White lists)

تحتوي القائمة السوداء على عناوين بريد إلكترونية، أو أسماء نطاقات (Domain Names) أو عناوين بروتوكول الانترنت (IP addresses)لخوادم بريد إلكترونية، لايُسمَح للرسائل الإلكترونية القادمة من تلك العناوين بالمرور من خلال الخادم المُستقبِل. فإذا تطابقت إحدى خصائص البريد الإلكتروني القادم مع أحد عناصر القائمة على الأقل فإنه يكون من القائمة السوداء، ولايُسمَح له بالمرور إلى بريد المُستقبِل.

(1) M. Gupta, C. Shue, "Spoofing and Countermeasures", Book chapter in "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft", edited by Jakobsson and Myers, 2006, Wiley.

بالإمكان إعداد خادم البريد الإلكتروني بالنسبة للمُستقبِل لتصفية الرسائل القادمة بالاعتماد على القوائم السوداء، وأيضاً يمكن إعداده لرفض الرسائل المصنفة من القائمة السوداء أو نقلها الى مجلد خاص في حساب المُستقبِل يعرف عادة بـ (Junk E-Mail) أو (Bulk) أو (Spam) وترك القرار في هذه الحالة للمُستقبِل إما بإبقاء الرسالة أو حذفها.

أما القوائم البيضاء فهي على العكس تماماً من القوائم السوداء. فالبريد القادم، حتى وإن طابق القائمة السوداء، يُسمَح له بالمرور إذا تطابقت إحدى خصائصه مع أحد عناصر القائمة البيضاء على الأقل، وذلك لضمان التأكد من وصول البريد القادم من أطراف مهمة إلى حساب بريد المُستقبِل، حتى وإن تم تصنيفه من ضمن القائمة السوداء. وهناك طريقة أخرى لاستخدام القوائم البيضاء هي السماح فقط لرسائل البريد القادمة من العناوين أو النطاقات أو الخوادم المحددة في القائمة البيضاء، وغير ذلك من الرسائل التي لم تصنف من ضمن القائمة البيضاء فإنه يتم رفضها أو إيصالها إلى المجلد الخاص في حساب المُستخدِم، كما في طريقة التصفية باستخدام القوائم السوداء.

بإمكان مدير الخادم - وبإعدادات متقدمة للخادم- حذف الرسائل المصنفة إيجابياً من القائمة السوداء أو نقلها إلى مجلد خاص في حساب المُستقبِل بناءاً على التقييم (scoring) حيث تُقَيَّم الرسالة الواردة بالنسبة لشروط القائمة السوداء، وبناء على درجة التقييم يتخذ الخادم القرار بحذف الرسالة أو نقلها. وعادة إذا كانت درجة التقييم عالية، أي إن معظم الشروط قد انطبقت على الرسالة، فإنه يتم رفضها أو حذفها. والعكس بالعكس. فإذا كانت درجة التقييم مُتدنِية، أي أن عدداً قليلاً من الشروط قد انطبق على الرسالة، فإنه يتم نقلها إلى المجلد الخاص في حساب المُستقبِل.

القوائم السوداء والقوائم البيضاء وحدها غير كافية للتصدي للرسائل غير المرغوبة، و إنما تساعد في التقليل منها إحصائياً. فالبنسبة للقوائم البيضاء فإنها تقلل من حدوث النتائج الإيجابية الكاذبة (false positives) بافتراض أن معظم الرسائل المرغوبة سترسل من مجموعة صغيرة ومُعرَّفة من المُرسِلين، وأيضاً استخدام القوائم البيضاء كمرحلة ثانية بعد القائمة السوداء في تصفية الرسائل.

3.3.2 الإجراء المضاد الثالث: القوائم البيضاء التجارية (Commercial Whitelists)

هي أنظمة قوائم تُباع بواسطة جهات مستقلة أو من مُقدِم خدمة البريد الإلكتروني مقابل مبلغ مالي يدفعه المُرسِل لضمان وصول بريده إلى المُستقبِل.

من الأساليب المستخدمة في مثل هذه الأنظمة هي التقييم (scoring)، والشهادات (certificates)، وبناء على ذلك ترخص الرسالة بأنها من مصدر موثوق، وتنجح بالمرور إلى بريد المُستقبِل.

4.3.2 الإجراء المضاد الرابع: التحقق من التكاملية (Integrity Check)

كما ذكرنا سابقاً أن برتوكول نقل البريد البسيط (SMTP) الذي يُستخدَم في تراسل البريد الإلكتروني على الشبكة العالمية يفتقد خاصية التصديق (Authentication)، وبالتالي عنوان المُرسِل. ليس بالضرورة أن يكون صحيحاً أو يعكس شخصية المُرسِل، فيمكن لأي شخص يضع في حقل المُرسِل أي عنوان بريد إلكتروني، وهذه الثغرة الأمنية تم استغلالها في إرسال الرسائل غير المرغوبة عن طريق الاحتيال (spoofing).

بالإمكان فحص الرسائل للتحقق من الكمالية عن طريق تحليل ترويسة رأس الرسالة (Header)، ومقارنة عنوان المُرسِل المذكور في حقل الـ "من" (From) مع القيمة الموجودة في ترويسة في الحقل "وارد" (Received). هذه الطريقة تساعد في اكتشاف الرسائل غير المرغوبة [1].

5.3.2 الإجراء المضاد الخامس: تحوير العنوان

كتابة العنوان البريدي في المواقع العامة، سواء كانت في صفحات الشبكة العالمية، أو غرف المحادثة، أو مجموعات النقاش، أو غيرها يجعلها عرضة لبرامج التجميع الآلية لعناوين البريد الإلكتروني التي تستخدم في إرسال البريد غير المرغوب. ولهذا ظهر إجراء تحوير عنوان البريد الإلكتروني لتفادي جمعها من مثل هذه البرامج إذا اضطر الشخص لكتابة عنوانه البريدي في المواقع العامة.

من الأمثلة على هذه الإجراء استبدال الكلمة: "at" بالرمز "@" والكلمة "dot"، بالنقطة "." مثال "xyz@abc.com" تصبح بعد التحوير "xyz at abc dot com"، وبهذه الطريقة لاتستطيع برامج تجميع عناوين البريد الإلكتروني الآلي من التعرف عليه، بالمقابل فإنها تكون قد أدت الغرض في ايصال العنوان.

من الأمثلة الأخرى لهذه الإجراء كتابة عنوان البريد الإلكتروني رمزاً نصياً في ملف صورة، وبالتالي يتعذر على برامج التجميع الآلية التعرف على العنوان.

6.3.2 الإجراء المضاد السادس: عدم الرد على الرسائل غير المرغوبة

كما ذكرنا في التعريف فإن الرسائل غير المرغوبة يتم إرسالها لعدد كبير (Bulk) من العناوين البريدية العشوائية على أمل وصولها، ولو على أقل تقدير، إلى بعض

(1) Technologies to Combat Spam, Thomas A. Knox, GIAC Security Essentials Certification (GSEC) Practical Assignment, Version 1.4b, Option 1, June 16, 2003, SANS Institute 2003.

هذه العناوين. الرد على الرسائل غير المرغوبة يعطي المُرسِل دلالة على أن الرد قادم من عنوان نشيط وحقيقي، فيستغله في رسائل مستقبلية أخرى غير مرغوبة.

بنفس الطريقة فإن بعض الرسائل غير المرغوبة تحتوي على رابط لإزالة عنوان المُستقبِل من القائمة البريدية للمُرسِل لإيقاف إرسال الرسائل المستقبلية الأخرى، قد يكون الهدف الحقيقي من وراء هذا الرابط هو تحديد ما إذا كان عنوان المُستقبِل نشيطاً أم لا.

أفضل طريقة للتعامل مع رسائل البريد غير المرغوبة هو عدم فتحها والإبلاغ عنها، كما سنرى في الإجراء المضاد السابع.

7.3.2 الإجراء المضاد السابع: الإبلاغ عن رسائل البريد غير المرغوبة (Spam Reporting)

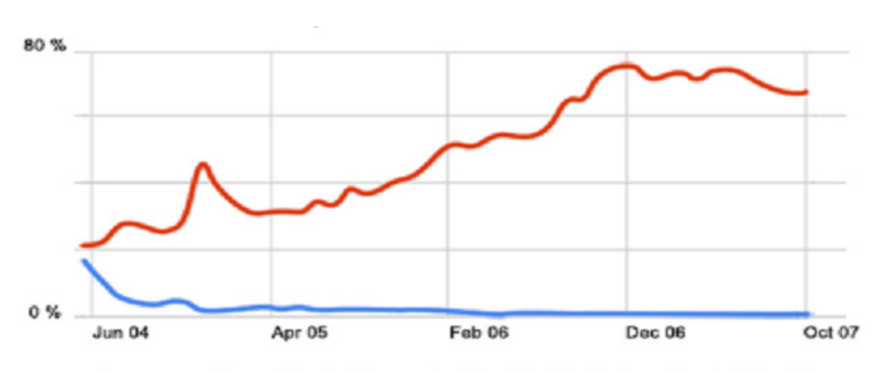
قد يساعد الإبلاغ عن رسائل البريد غير المرغوبة في التقليل منها والتصدي لها. يتم الإبلاغ عن هذه الرسائل بالاتصال بمقدم خدمة البريد الإلكتروني لمُرسِل الرسالة غير المرغوبة. يمكن التعرف على مقدم الخدمة من اسم النطاق في العنوان البريدي للمُرسِل. وكما تم ذكره سابقاً فإن اسم النطاق هو الجزء الذي يأتي بعد علامة: "@" في عنوان البريد الإلكتروني. فمثلاً اسم النطاق للعنوان البريدي "xyz@abc.com" هو "abc.com" بالإمكان الحصول على بيانات الاتصال لأي اسم نطاق من خادم "WHOIS" [1] – ترجمته بالغة العربية "من يكون؟" - ، هذا الخادم يحوي قاعدة بيانات تسجيل النطاقات.

(1) للاتصال بهذا الخادم يلزم وجود واجهة استخدام إما عن طريق تطبيق مخصص للاستعلام، أو عن طريق أحد المواقع على الشبكة العالمية التي تقدم خدمة الاستعلام مثل موقع: (whois.net).

هناك مستوى آخر للإبلاغ هو إبلاغ مُقدِم خدمة البريد الإلكتروني الذي يتعامل معه صاحب البريد المُستقبِل. من طرق الإبلاغ المستخدمة تخصيص أحد الأزرار في واجهة المُستخدِم في عميل البريد الإلكتروني للإبلاغ. عندما تتجمع عند الخادم بلاغات كثيرة على البريد نفسه فإنه يتخذ إجراءات خاصة، منها إبلاغ الخادم مُصدِّر الرسالة، أو وضع عنوان المُرسِل في القائمة السوداء، فلا يتمكن مستقبلاً من إرسال رسائل أخرى.

هذه الطريقة المضادة للرسائل غير المرغوبة فعالة إلى حد معين، ويتاح للمُرسِل من خلالها الانتقال إلى مقدم خدمة آخر، وبالتالي استخدام اسم نطاق آخر.

يوضح الرسم البياني 1 في الشكل (2- 1) المعد من قبل خدمة البريد الإلكتروني (Gmail) 2 ، نسبة البريد غير المرغوب القادم إلى الخادم قبل التصفية،



شكل (2–1) نسبة البريد غير المرغوب القادم إلى الخادم قبل التصفية ونسبة البريد غير المرغوب المُبَلَغ عنه

(المصدر gmail.com)

(1) mail uses Google's innovative technology to keep spam out of your inbox", gmail.com, (http://www.google.com/mail/help/fightspam/spamexplained.html), December, 2007.

(2) مقدم خدمة بريد إلكتروني مبني على الشبكة العالمية (gmail.com) .

ونسبة البريد غير المرغوب المبلغ عنه من قبل المُستقبِلين.

وكما يُظهِر الرسم البياني فإن نسبة البريد غير المرغوب المبلغ عنه تشكل أقل من 1٪ من إجمالي عدد الرسائل غير المرغوبة.

8.3.2 الإجراء المضاد الثامن: التقيد بوثيقة طلب التعليقات لبرتوكول نقل البريد البسيط (SMTP RFC)

قد يُستخدَم التحقق من المتطلبات الفنية لبروتوكول نقل البريد البسيط (SMTP) في البريد الوارد للتقليل من الرسائل غير المرغوبة القادمة من الخوادم التي لاتتقيد بهذه المتطلبات. العديد من مُرسِلي البريد غير المرغوب يستخدمون برامج رديئة ، أو ليس باستطاعتهم التقيد بالمتطلبات الفنية لبروتوكول نقل البريد البسيط (SMTP) لقلة التحكم لديهم في الخادم الذي يرسلون منه والذي عادة مايكون جهاز ضحية تم اختراقه من قبل مخربين (Hackers).

9.3.2 الإجراء المضاد التاسع: سجلات تبادل الرسائل المزيفة (Fake MX Records)

أحد الإجراءات المضادة الفعَّالة في التصدي لرسائل البريد الإلكتروني غير المرغوبة هو وضع سجلات تبادل رسائل مزيفة عند رد خادم أسماء النطاقات على طلب استعلام عن خوادم البريد الإلكتروني لاسم نطاق.

وكما ذكرنا في فصل : "نظام البريد الإلكتروني" فإن هناك رقما تفضيلياً مع كل سجل في الرد ، وأن الغرض من هذا الرقم هو ترتيب الخوادم. فكلما كان رقم التفضيل أصغر كانت احتمالية النجاح أكبر في توصيل الرسالة. ولهذا فإن الخادم

المُرسِل يحاول الاتصال أولاً مع الخادم ذي الرقم الأدنى، فإن لم ينجح الاتصال معه لسبب ما فإنه يحاول مع الخادم الذي يليه.

هناك نوعان من السجلات المزيفة بالاعتماد على الرقم التفضيلي للسجل:

- **سجل تبادل الرسائل الأدنى المزيف**

(Fake Lowest MX Record)

نظراً لطبيعة رسائل البريد الإلكتروني غير المرغوبة في كونها تُرسَل بأعداد كبيرة، وفي أغلب الأحيان لا يهتم مُرسِلوها بإعادة محاولة الاتصال بخادم البريد الإلكتروني في حال فشل الاتصال، بل ينتقلون إلى العنوان البريدي التالي.

يتصدى تضمين سجل تبادل مزيف برقم تفضيلي أصغر من كل السجلات في الرد من قبل خادم أسماء النطاقات على طلب الاستعلام عن خوادم البريد الإلكتروني لاسم نطاق معيّن بشكل فعّال للرسائل غير المرغوبة.

يجب أن يؤشر سجل تبادل الرسائل الأدنى المزيف إلى عنوان خادم نشيط بحيث يكون المنفذ رقم 25 (Port 25)لهذا الخادم مغلقاً لضمان استلام الرسائل المرغوبة فقط عبر الخوادم الأخرى.

- **سجل تبادل الرسائل الأعلى المزيف**

(Fake Highest MX Record)

قد يبتديء مُرسِلو الرسائل غير المرغوبة محاولة الاتصال مع الخادم ذي الرقم التفضيلي الأعلى بدلاً من الخادم ذي الرقم التفضيلي الأدنى لاحتمال كبير هو كون الخادم ذي الرقم التفضيلي الأعلى خادماً احتياطياً مع برامج أقل فاعلية لمكافحة

الرسائل غير المرغوبة مقارنة مع الخوادم الأخرى.

تضمين سجل تبادل مزيف برقم تفضيلي أعلى من كل السجلات في الرد من قِبَل خادم أسماء النطاقات على طلب الاستعلام عن خوادم البريد الإلكتروني لاسم نطاق كفيل بالتصدي لهذا الأسلوب في إرسال الرسائل غير المرغوبة.

سجل تبادل الرسائل الأعلى المزيف قد يكون غير معرّف، أو يشير إلى عنوان بروتوكول انترنت خامل (dead IP address)، أو يوشر إلى عنوان خادم حقيقي بحيث يكون المنفذ رقم 25 (Port 25)لذلك الخادم مغلقاً.

يكون تطبيق كلا النوعين من السجلات المزيفة إجراء مضاداً أفضل، كما في الشكل(2- 2).

سجل مزيف →	10	fake1.xyz.com
سجل حقيقي →	20	mail1.xyz.com
سجل حقيقي →	30	mail2.xyz.com
سجل حقيقي →	40	mail3.xyz.com
سجل مزيف →	50	fake2.xyz.com

شكل (2–2) مثال على سجلات تبادل الرسائل المزيفة

10.3.2 الإجراء المضاد العاشر: تأخير الترحيب (Greeting delay)

هو تأخر متعمد لفترة قصيرة من قبل خادم البريد الإلكتروني المُستقبل قبل الرد على طلب الاتصال من خادم بريد إلكتروني آخر.

طبقاً للمواصفات الفنية لبرتوكول نقل البريد البسيط (SMTP)، فإنه بعد

طلب الاتصال فإنَّ على الخادم المُرسِل الانتظار لحين استقبال رسالة الترحيب من الخادم المُستقبِل قبل إرسال البريد الإلكتروني إليه.

يمكن الاستفادة من فترة التأخر هذه للتصدي للرسائل غير المرغوبة، كون مُرسِليها عادة لاينتظرون رسالة الترحيب، بل يرسلون مباشرة بعد طلب الاتصال.

بالإمكان إعداد الخادم لاكتشاف هذه الطريقة، ومن ثم قطع الاتصال مع الخادم المُرسِل.

الفصل الثالث
الاصطياد الإلكتروني
(Phishing)

يناقش هذا الفصل الاصطياد الإلكتروني من حيث تعريفه، وأهدافه، والأضرار المترتبة عليه على مستوى الأفراد والمنظمات.

تعني رسائل الاصطياد الإلكتروني (Phishing): سرقة البيانات الشخصية السرية والحساسة عن طريق رسائل البريد الإلكتروني لغرض انتحال الشخصية، وذلك عن طريق انتحال شخصية أحد المصارف، أو منظمة معينة وإيهام الضحية بجدية الطلب وأهميته.

سمي هذا النوع من الرسائل رسائل الاصطياد الالكتروني لأن مُرسِليها يستخدمون رسالة البريد الإلكتروني كطعماً لاصطياد الأرقام السرية وغيرها من البيانات الشخصية الحساسة الأخرى من بحر مستخدمي الشبكة العالمية.

كما هي الحال في الرسائل الإلكترونية غير المرغوبة (Spam)، فإن رسائل الاصطياد الإلكتروني لاتقتصر على البريد الإلكتروني فقط، بل تتعداها إلى تطبيقات التراسل الإلكترونية الأخرى كالرسائل النصية القصيرة (SMS) والرسائل الآنية أو المباشرة (Instant Messaging)، كون المفهوم يبقى نفسه، ولكن الاختلاف يكون في الوسيط الذي يتم تنفيذ الجريمة من خلاله. لكن رسائل البريد الإلكتروني هي الأكثر شيوعاً في تنفيذ هجمات الاصطياد الالكتروني 1.

كان أوائل مخترقي الشبكة العالمية (Hackers) عادة مايستبدلون الحرفين "ph" بالحرف "f" لإنشاء كلمات جديدة في مجتمعهم، أي مجتمع قراصنة الشبكة العالمية، كون النطق هو نفسه، ولكن الكتابة تختلف. نشأت كلمة (Phishing) في تسعينات القرن العشرين من الكلمة (fishing) التي تعني اصطياد السمك.

رسائل الاصطياد الإلكتروني مثلها مثل الرسائل البريدية غير المرغوبة (Spam)

(1) A. Emigh, "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures", Radix Labs, October 3, 2005.

كـون مُرسِليها أيضـاً يسـتغلون الجانـب الاجتمـاعي، بالإضـافة إلى الجانـب الفـني في عمليـة الاحتيـال علـى الضـحية، وهـذا كمـا ذكـر سـابقاً ينـدرج تحـت بـاب الهندسـة الاجتماعية (Social Engineering).

يدَّعي مُرسِلو رسـائل الاصـطياد الإلكترونيـة أن مصـدرها منظمـات حقيقيـة، كالمصـارف الماليـة في محاولـة لخـداع مُسـتقبِل هـذا البريـد لإفشـاء بياناتـه الشخصـية، كبيانات الدخول علـى الحسـاب الشخصـي في مصـرف مـا، كاسـم المُستخدِم، ورمـز التعريـف الشخصـي، أوبيانـات البطاقـات الائتمانيـة كبطاقـة فيـزا (VISA) الائتمانيـة لغرض سرقتها، وانتحال شخصية الضحية لاحقاً.

مثال تقليدي لرسائل الاصطياد الالكتروني، رسـالة بريـد إلكترونـي تـدّعي أن مصدرها المصرف "س". وكما ذُكِر سابقاً فإن برتوكـول نقـل البريـد البسـيط (SMTP) يفتقـد خاصـية التصـديق (Authentication)، كـون عنـوان المُرسِـل لـيس بالضـرورة أن يعكس حقيقة شخصية المُرسِل، لأنه يمكـن التلاعـب بحقـل عنـوان المُرسِل. وفي هـذا المثال يضع المُرسِل عنواناً بريدياً ملّفقاً متبوعـاً باسـم النطـاق لـذلك المصـرف، لإيهـام المُستقبِل بأن مصـدرها هـو المصـرف "س". وعـن طريـق اسـتخدام رسـائل البريـد غـير المرغوبة (Spam) ترسل هذه الرسالة لعدد هائل من عناوين البريد الإلكترونية.

سـوف يكتـب محتـوى هـذه الرسـالة بطريقـة لخـداع المُسـتقبِل لإفشـاء بيانـات الدخول إلى حسابه الشخصي عبر الموقع الإلكترونـي لـذلك المصـرف، وذلـك بكتابـة الرسالة بطريقة مشابهة لـنمط (Style) رسـائل المصـرف البريديـة الموجهـة للعمـلاء مـن حيث النظر والإحساس (Look and Feel)، ووضـع رمـز المصـرف (Logo)، وشـعاره (slogans).

أحد أساليب الخداع التي استُخدِمت في كتابة محتوى الرسالة هـو الادعـاء بـأن

محاولات الدخول إلى الحساب الشخصي للمُستقبل قد استنفدت، وأنه لابد من تعبئة النموذج الموجود في الرابط الموجود بالرسالة، ويكون هذا الرابط لموقع مزور (Spoofed) مصمم ليطابق تصميم موقع المصرف الأصلي من حيث أيضا النظر والإحساس (Look and Feel)، ووضع اسم المصرف ورمزه وشعاره، كون هيئة اللغة الأساسية لإنشاء المواقع الإلكترونية، ألا وهي لغة الترميز النصي المتشعب (Hypertext Markup Language – HTML)، تجعل وطبيعتها- نسخ الصور من المواقع الإلكترونية الأخرى، أو حتى نسخ الموقع الإلكتروني بكامله أمراً سهلاً، والهدف من ذلك هو محاولة خداع المُستقبل الذي صادف أنه عميل لذلك المصرف، وذلك بسرقة بيانات الدخول إلى الحساب الإلكتروني التي عادة ماتكون اسم المستخدم، ورمز التعريف الشخصي.

قد تكون رسالة البريد الإلكترونية نفسها مزودة بنموذج (form)، ويطلب من المُستقبل تعبئته، ومن ثم ارسالها مرة أخرى إلى المُرسِل، أو بتسليم النموذج بالبيانات المعبئة فيه إلى عنوان موقع على الشبكة العالمية في حالة البريد الإلكتروني المبني على الشبكة العالمية (Web-based E-Mail – webmail).

في المثال السابق نجد أن الرسالة البريدية مثَّلَت الطعم الذي جذب الضحية، والذي كما ذكرنا أنه صادف أن يكون عميلاً لدى ذلك المصرف، بينما مَثَّلَ الموقع المزور كُلاب الصنارة الذي تم اصطياد الضحية بواسطته.

من الوسائل الأخرى المشهورة المستخدمة في رسائل الاصطياد الالكتروني [1]:

- رسالة تدّعي أن هناك مشكلة في حساب المُستقبل في مصرف ما، وتطلب من

(1) A. Emigh, "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures", Radix Labs, October 3, 2005.

المُستقبِل زيارة موقع لتصحيح المشكلة باستخدام رابط لموقع مزور موجود في الرسالة.

- رسالة تدّعي أن حساب المُستقبِل في مصرف ما في خطر، وتعرض عليه التسجيل في برنامج مكافحة الاختلاسات.

- رسالة فاتورة مبيعات، وهي في الأصل مزيفة، ولم يقم المُستقبِل بطلبها، ويزود المُستقبِل برابط موجود في الرسالة لإلغاء هذا الطلب المزيف.

- رسالة إشعار مزيف بحصول تغيير غير متوقع على الحساب المصرفي للمُستقبِل، ويزود المُستقبِل برابط للنظر في هذا التغيير.

- رسالة تدّعي نزول خدمات مالية جديدة في مصرف ما، وتعرض على المُستقبِل، كونه عميلاً حالياً فرصة الحصول على هذه الخدمة مجاناً لفترة مؤقتة.

في كل حالة من الحالات السابقة فإن مُستقبِل الرسالة يوجه إلى موقع مزور لجمع البيانات السرية، والتي يستخدمها "الصيادون" لاحقاً في انتحال شخصية الضحية في عمليات إما مالية أو أخرى.

يمكن اختصار هجمات الاصطياد الالكتروني في الخطوات التالية:

1- التخطيط لهجمة الاصطياد الالكتروني.
2- تجهيز الموقع المزيف.
3- إرسال كمية هائلة من الرسائل المزيفة، وقد تكون باستخدام أحد أساليب الرسائل غير المرغوبة (Spam).
4- عدد من المُستقبِلين للرسالة المزورة يقومون بفتح الرسالة، وتتبع الرابط الموجود في الرسالة، ومن ثم كتابة البيانات المطلوبة في الموقع المزيف.
5- الصيادون يسرقون البيانات السرية، ومن ثم ينتحلون شخصيات الضحايا.

من الأمثلة 1 الواقعية لهجمات الاصطياد الالكتروني رسالة البريد الإلكتروني، كما في الشكل (3-1)، التي زعم مُرسِلها أنها من "قسم الأمان" في مصرف "سامبا"، وأن المُستقبِل مدعو لاجتياز ماسموه: "عملية الترخيص" ووضعوا رابطاً للانتقال إلى صفحة الترخيص تلك والذي اتضح أن هذه الصفحة هي موقع مزيف مطابق لتصميم موقع "سامبا" الأصلي من ناحية النظر والإحساس (look and feel) والنمط (style)، ووضع رمز المصرف كما في الشكل (3-2).

عميلنا العزيز،
يود قسم الأمان في البنك لدينا أن يخطرك بأنه تم اتخاذ بعض الإجراءات للارتقاء بمستوى الأمان في تعاملاتك البنكية عبر الإنترنت، وذلك لمواجهة المحاولات المستمرة لاختراق الحسابات البنكية بصورة غير قانونية.للوصل إلى النسخة الأكثر أماناً من منطقة العملاء، يرجى اجتياز عملية الترخيص. **انقر هنا** للانتقال إلى صفحة الترخيص نود أن نحيطكم علماً بضرورة التعامل مع إجراءات الأمان الجديدة بصورة جدية للغاية والاطلاع عليها الآن.مع أطيب الأمنيات، قسم الأمان

شكل (3-1) رسالة الاصطياد الالكتروني المنتحلة لمصرف "سامبا"

(1) "وقفة تحليلية لحادثة رسالة الاصطياد الالكتروني الموجهة لعملاء احد البنوك السعودية"، خالد الغثبر، جريدة الرياض السعودية، السبت 14 من ذي الحجة 1426هـ - 14 يناير 2006م - العدد 13718.

إذا دققنا في اسم النطاق للمصرف نجد أن الصيادين عمدوا إلى وضعه قريباً من اسم النطاق الصحيح ، كي يَصعُب على العميل الضحية اكتشافه من الوهلة الأولى. اسم النطاق الصحيح لمصرف سامبا هو (samba.com) بينما كان اسم النطاق للموقع المزور هو (sambaonlineaccess.com) نجد في اسم النطاق للموقع المزور ذكر اسم المصرف، وذكر (onlineaccess) ، وتعني الاتصال المباشر، مما يوحي ويعطي انطباعاً بشرعية الموقع.



شكل (3–2) الموقع المزيف لمصرف "سامبا"

الشكل (3-3) هو لموقع سامبا الأصلي، ونجد مدى التشابه بين الموقع المزور والموقع الأصلي.

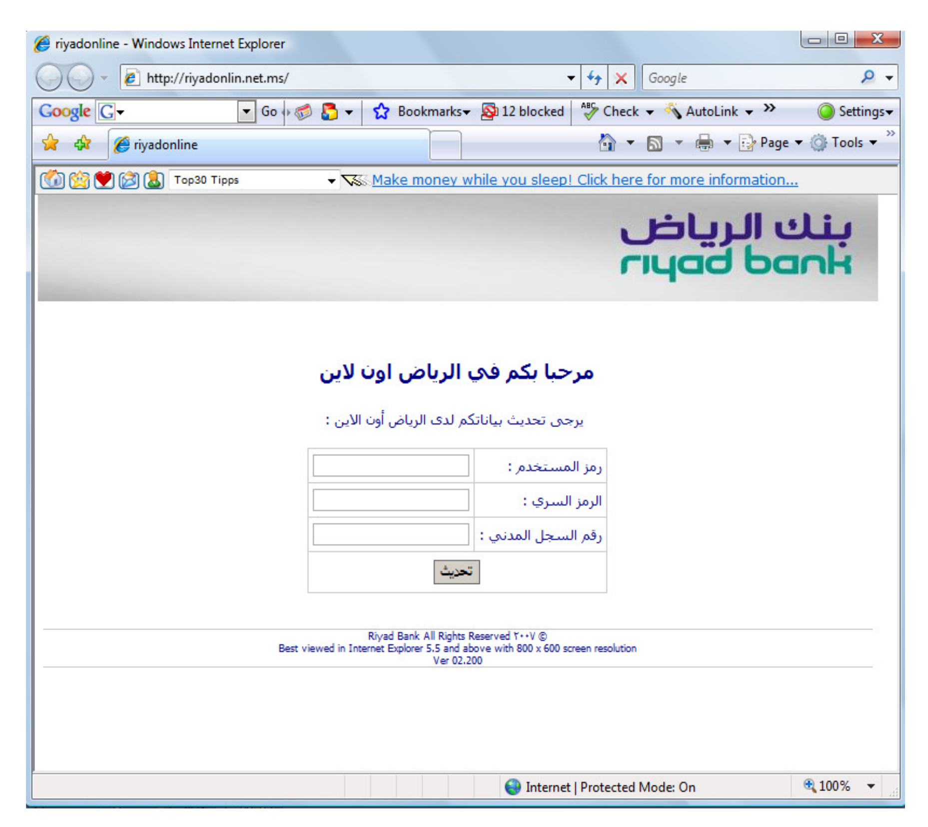


شكل (3-3) الموقع الأصلي لمصرف "سامبا"

مثال آخر لموقع مزور هو موقع مصرف "الرياض". ونلاحظ أيضاً أن الموقع المزور كما في الشكل (3-4) صمم ليطابق الموقع الأصلي للمصرف كما في الشكل (3-5) من حيث الشعار، والنمط، والنظر والإحساس.

اسم النطاق للموقع الأصلي هو: (riyadbank.com)، واسم النطاق للموقع المزيف (riyadonlin.net.ms).

سنناقش في فصل : "أساليب الاصطياد الإلكتروني" بشكل مفصل أساليب الاحتيال في تزوير المواقع ؛ وسنناقش في جزء الإجراءات المضادة الاحتياطات والدلائل المختلفة لاكتشاف المواقع المزورة.



شكل (3–4) الموقع المزيف لمصرف "الرياض"



شكل (3-5) الموقع الأصلي لمصرف "الرياض"

ويظهر الشكل (3-6) مثالاً آخر لمواقع الاصطياد الالكتروني، وهذا المثال لمصرف "ساب". حمل الموقع المزور اسم النطاق (sabb.net.ms) المشابه لاسم النطاق للموقع الأصلي (sabb.com)، كما في الشكل (3-7). ونرى أيضاً أن الموقع المزور صمم ليطابق الموقع الأصلي من حيث النمط، والشعار، والنظر والإحساس.



شكل 3–6 الموقع المزيف لمصرف "ساب"



شكل(3–7) الموقع الأصلي لمصرف "ساب"

في دراسة [1] شملت مراقبة غرف المحادثة (chat rooms) ورصدها على الشبكة العالمية التي كان يحل فيها الصيادون (phishers)، أظهرت أن هجمات الاصطياد الالكتروني بشكل عام لا تُنفَذ من قِبَل شخص واحد، بل إن وراء هذه الهجمات أشخاص كثر كل متخصص في مجال معين لمساعدة كل من الصيادين (phishers) ومُرسِلي الرسائل غير المرغوبة (spammers)، والمخرِّبين (hackers) في تعزيز تلك الهجمات. وجدت هذه الدراسة أنه كانت هناك عدة مجموعات من العمال المتخصصين كالمُرسِلين (mailers) والمجمعين (collectors) والمحصلين (cashers)، كما هو معرَّف في التالي:

- المُرسِلون (Mailers): وهم إما مُرسِلو الرسائل غير المرغوبة (spammers) أو المُخرِّبون (hackers)، الذين لديهم القدرة على إرسال عدد هائل من الرسائل غير المرغوبة بهدف الاحتيال (fraudulent emails).

- المجمعون (Collectors): هم المخرِّبون (hackers) الذين جهزوا المواقع الإلكترونية المزيفة (fraudulent websites) لغرض الاحتيال، والتي يتم تحويل الضحايا إليها من قِبَل الرسائل البريدية غير المرغوبة بعدما تطلب منهم هذه المواقع تزويد بيانات سرية كإسم المستخدم، ورقم المرور، أو رقم البطاقة الائتمانية.

ولاحظت الدراسة أن المجمِّعين هم عملاء متكررون عند المُرسِلين (mailers)، وهم يدفعون مبلغاً مادياً لإرسال الرسائل غير المرغوبة.

- المحصِّلون (Cashers): وهم الذين يقومون بأخذ البيانات السرية المسروقة

---

(1) Christopher Abad, "The economy of phishing: A survey of the operations of the phishing market", First Monday, volume 10, number 9, September 2005, (http://firstmonday.org/issues/issue10_9/abad/index.html). M. Jakobsson, S. Myers, "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft", Wiley, 2007.

من قبل المجمِّعين، ومن ثَم استغلالها. و ينفذ الاستغلال بعدة طرق كإنشاء بطاقات حسابات ائتمان مزيفة، أو بطاقات حسابات مصرفية مزيفة تستخدم للسحب النقدي المباشر من أجهزة الصرَّاف الآلي (Automated Teller Machine – ATM)، أو الشراء والبيع بواسطتها.

وهؤلاء المُحصِّلون معروفون إما بالدفع المادي المباشر إلى المجمعين لقاء البيانات السرية المسروقة، أو بإعطائهم نسبة من المسروقات النقدية المحصلة. المبالغ المادية المدفوعة سواء مباشرة أو عن طريق النسبة تعتمد على جودة البيانات المزودة وكميتها من قِبَل المُجمِّعين ، وتعتمد أيضاً على قدرة المحصلين على الهجمات والاحتيالات المنفذة على مختلف المنظمات المتعلقة ببيانات حسابات المستخدمين المجمعة.

إلى هنا خلصت الدراسة التي أوضحت أن هجمات الاصطياد الالكتروني تقف وراءها عصابات منظمة مطابقة لتنظيم العصابات الإجرامية في العالم، إلا أنها تختلف عنها فقط في أن تنفيذها يتم في العالم الإلكتروني، أي عالم الشبكة العالمية (Internet world).

الشيء الاستثنائي في رسائل الاصطياد الالكتروني أنها تقدم عاملاً جديداً من عوامل الهجمات الأمنية الإلكترونية، وهو ما تم تجاهله غالباً في الاحتياطات والدفاعات الأمنية في المنظمات، ألا وهو العامل البشري. فجدران الحماية (Firewalls)، والشهادات الأمنية (Secure Socket Layer – SSL Certificates)، وقوانين أنظمة منع الاختراق (Intrusion Prevention Systems – IPS rules)، وغيرها من وسائل الحماية الأمنية الباهظة التكلفة لايمكن أن توقف استغلال الوثوق الآني (online trust) عبر الشبكة العالمية بين العميل والمنظمة، والتي لايتوقف ضررها عند

تسرب بيانات العميل الشخصية والسريّة فقط، بل يتعداها إلى إحداث ضرر كبير في ثقة العميل بوسائل الاتصال المختلفة، سواء عبر الشبكة العالمية أو نظام الرد الآلي عبر الهاتف، أو غيرهم من وسائل الاتصال بين العميل والمنظمات.

مجموعة عمل التصدي لرسائل الاصطياد الإلكتروني (The Anti-Phishing Working Group – APWG) [1]. هي جمعية عالمية على مستوى مختلف الصناعات هدفها إنفاذ القوانين للتصدي لعمليات الخداع وانتحال الشخصية الناتجة عن رسائل الاصطياد الإلكتروني.

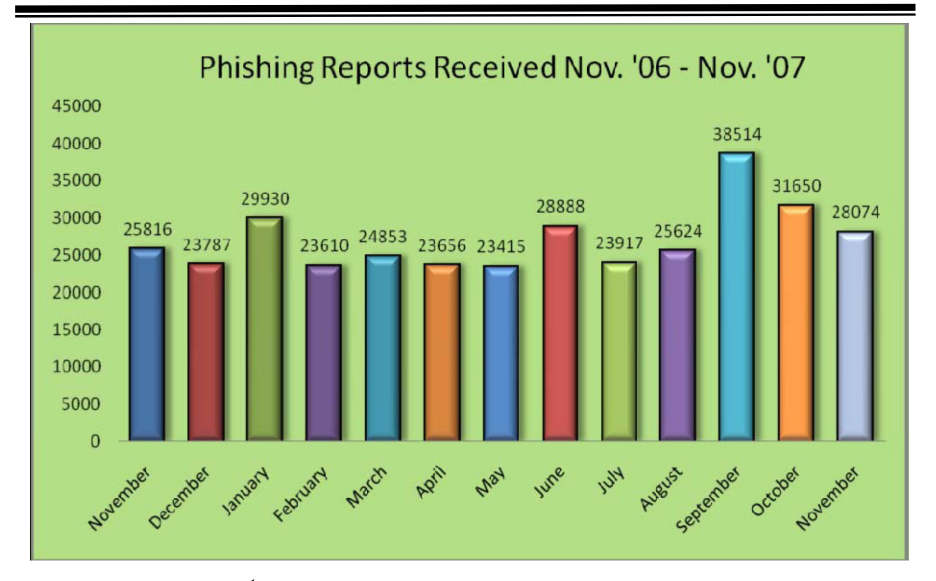
في تقرير [2] شهر نوفمبر من عام 2007 الذي أعدته مجموعة عمل التصدي لرسائل الاصطياد الإلكتروني (APWG) أظهر أن المجموعة استقبلت في ذلك الشهر:

- 28074 بلاغاً عن رسائل اصطياد.
- 23630 بلاغاً عن مواقع إلكترونية مزيفة عن مواقع إلكترونية لمنظمات حقيقية.
- 178 علامة تجارية تم تزييفها (brand hijack) عن طريق حملات رسائل الاصطياد الالكتروني. وهذا الرقم أعلى رقم مسجل في شهر واحد، حتى وقت إصدار التقرير لذلك الشهر.
- 34.3٪ من مجموع رسائل الاصطياد الالكتروني المبلغ عنها احتوت على روابط لمواقع إلكترونية على هيئة أسماء نطاقات (domain names). مثال (xyzbank.com).

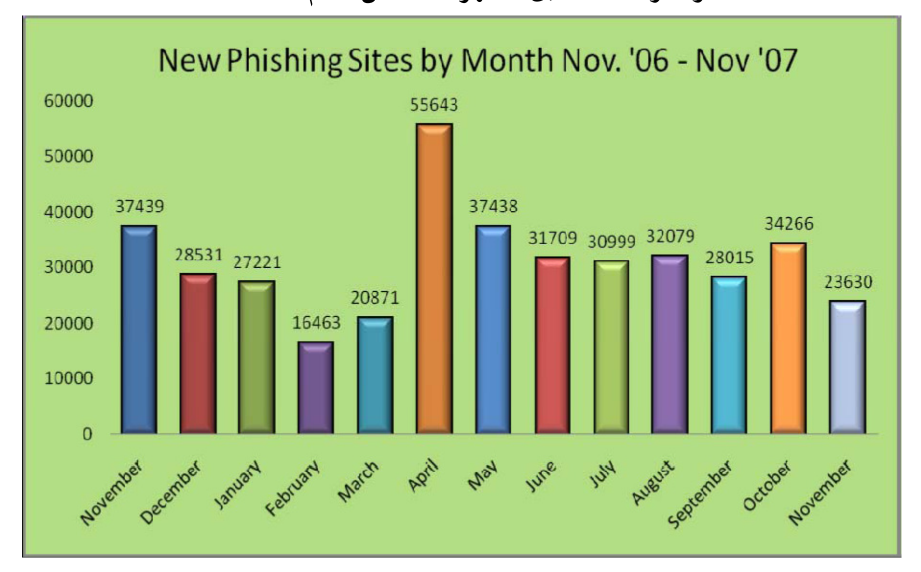
---

(1) The Anti-Phishing Working Group, www.apwg.com.
(2) Phishing Activity Trends, Report for the Month of November, 2007, Anti-Phishing Working Group (APWG), apwg.org

- 6٪ من مجموع رسائل الاصطياد الالكتروني المبلغ عنها احتوت على روابط لمواقع إلكترونية على هيئة عناوين عشرية. مثال (10.212.21.33).
- ثلاثة أيام هو معدل بقاء الموقع المزيف قبل إغلاقه.
- 30 يوماً هي أطول مدة بقاء لموقع مزيف.
- ازدياد عدد المنظمات المالية المستهدفة في الشرق الأوسط في عمليات تزييف العلامة التجارية.
- تظل المنظمات المالية الأكثر استهدافاً بما نسبته 93.8٪من إجمالي الصناعات الأخرى المستهدفة.
- في ذلك الشهر تخطت الصين الولايات المتحدة الأمريكية في عدد الخوادم المستضيفة لمواقع الاصطياد الإلكترونية بما نسبته 24.21٪
- يبين الشكل التوضيحي (3-8) عدد بلاغات الاصطياد الالكتروني المستلمة شهريا خلال الفترة من شهر نوفمبر 2006 إلى الشهر نفسه من العام 2007.
- يبين الشكل التوضيحي (3-9) عدد مواقع الاصطياد الالكتروني الجديدة المكتشفة شهرياً خلال الفترة من نوفمبر 2006 إلى الشهر نفسه من العام 2007.
- يبين الجدول (3-1) النسبة لكل نوع من أنواع المنظمات من حيث استهداف عمليات الاصطياد الالكتروني لها.
- يبين الجدول (3-2) الدول العشر الأولى في نسبة استضافة مواقع الاصطياد الإلكترونية.



شكل (3–8) عدد بلاغات الاصطياد الالكتروني المستلمة شهرياً خلال الفترة من شهر نوفمبر 2006 إلى الشهر نفسه من العام 2007



شكل (3–9) عدد مواقع الاصطياد الالكتروني الجديدة المكتشفة شهرياً خلال الفترة من نوفمبر 2006 إلى الشهر نفسه من العام 2007

جدول (3-1) قائمة النسب لكل نوع من أنواع المنظمات من حيث استهداف عمليات الاصطياد الالكتروني لها

النسبة (٪)	نوع المنظمة
93.8	الخدمات المالية (Financial Services)
2.8	البيع بالتجزئة (Retail)
2.2	مزودو خدمة الشبكة العالمية (ISP)
1.2	الحكومة وبقية الصناعات الأخرى (Government & Miscellaneous)

جدول (3-2) قائمة الدول العشر الأولى في نسبة استضافة مواقع الاصطياد الإلكترونية

النسبة (٪)	الدولة	الترتيب
24.21	الصين	1
23.85	الولايات المتحدة الأمريكية	2
9.39	الهند	3
8.06	روسيا	4
4.64	تايلند	5
3.53	رومانيا	6
3.41	ألمانيا	7
2.42	كوريا الجنوبية	8
1.47	المملكة المتحدة	9
1.47	فرنسا	10

في خبر 1 من (Gartner) أظهر أن الخسائر في الولايات المتحدة الأمريكية الناتجة من هجمات الاصطياد الالكتروني قد ارتفعت لتصل في عام 2007 إلى 3.2 بلايين دولار أمريكي. وأظهر التقرير أيضاً ارتفاعاً في هجمات الاصطياد الالكتروني على حسابات البطاقات الجارية والحسابات المصرفية، مقارنة بحسابات البطاقات الإئتمانية ويرجع السبب إلى ضعف أنظمة اكتشاف عمليات الاحتيال عند المصارف عنها بالنسبة إلى شركات البطاقات الائتمانية.

وذكر الخبر أيضاً أنه بناءاً على استطلاع أجري في شهر أغسطس من عام 2007 لأكثر من 4500 شخص في الولايات المتحدة الأمريكية تبين أن هجمات الاصطياد الالكتروني حققت نجاحاً أكبر في العام 2007، مقارنة بالعامين السابقين، قالت نسبة 3,3٪. من الأشخاص الذين استقبلوا رسائل اصطياد عن طريق البريد الإلكتروني إنهم تعرضوا لخسائر مالية بسبب رسائل الاصطياد الالكتروني، مقارنة بـ 2.3٪ تعرضوا للشيء نفسه في العام الذي سبقه، أي 2006، ومقارنة أيضا بـ 2.9 من العام 2005 بناءاً على استطلاعات مشابهة أجريت من قبل (Gartner).

وذكر الخبر أيضاً أن "PayPal"2، والتي تصنف من قطاع الخدمات المالية، و"eBay" 3، والتي تصنف من قطاع البيع بالتجزئة استمرتا لتكونا الأكثر تعرضاً لعمليات انتحال العلامة التجارية (brand spoofing).

هناك نوعان من هجمات الاصطياد الالكتروني، الأول هو النوع المُعتمِد على

(1) Media Relations, 2008 Press Releases, Gartner, "Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks", 05-March-2008, (http://www.gartner.com/it/page.jsp?id=565125).

(2) شركة متخصصة في المدفوعات والتحويلات المالية الإلكترونية.

(3) شركة متخصصة في البيع بالتجزئة عن طريق الشبكة العالمية.

الهندسة الاجتماعية (Social Engineering). في هذا النوع يستغل الصيادون - كما ذكرنا الجانب- البشري في عمليات الاصطياد الالكتروني باستخدام بريد انتحال الشخصية (spoofed email) لتوجيه المُستقبل إلى المواقع المزورة المصممة لتطابق مواقع أصلية، أو تعبئة نموذج مرفق مع الرسالة لخداع المُستقبل لإفشاء البيانات الشخصية والسرية.

النوع الآخر من هجمات الاصطياد الالكتروني هو النوع المعتمد على الأساليب الفنية (technical subterfuge)، ويقوم الصيادون في هذا النوع بزرع برامج تجسس (Spyware) في أجهزة الضحايا تتم من خلالها سرقة البيانات الشخصية والسرية، وإرسالها إلى الصيادين حيث يستخدمونها لاحقاً في عمليات انتحال الشخصية 1.

---

(1) Anti-Phishing Working Group, apwg.org.

الفصل الرابع
أساليب الاصطياد الإلكتروني
(Phishing Techniques)

- تسميم خادم أسماء النطاقات (DNS Poisoning)
- تسميم ملف الخوادم المضيفة (Hosts File Poisoning)
- الاصطياد الالكتروني بواسطة حقن المحتوى (Content Injection)
- هجمة الرجل في الوسط (Man-in-the-Middle Attack – MITM)
- تشويش العنوان (Address Obfuscation)
- الاصطياد الالكتروني عن طريق البرامج الخبيثة (Malware Attack)
- الاصطياد الالكتروني عن طريق محركات البحث (Search Engine Phishing)
- الاصطياد الالكتروني عن طريق النوافذ المنبثقة (The Popup Attack)
- شريط العنوان المزيف (Fake Address Bar)

يناقش هذا الفصل الأساليب المستخدمة في الاصطياد الإلكتروني.

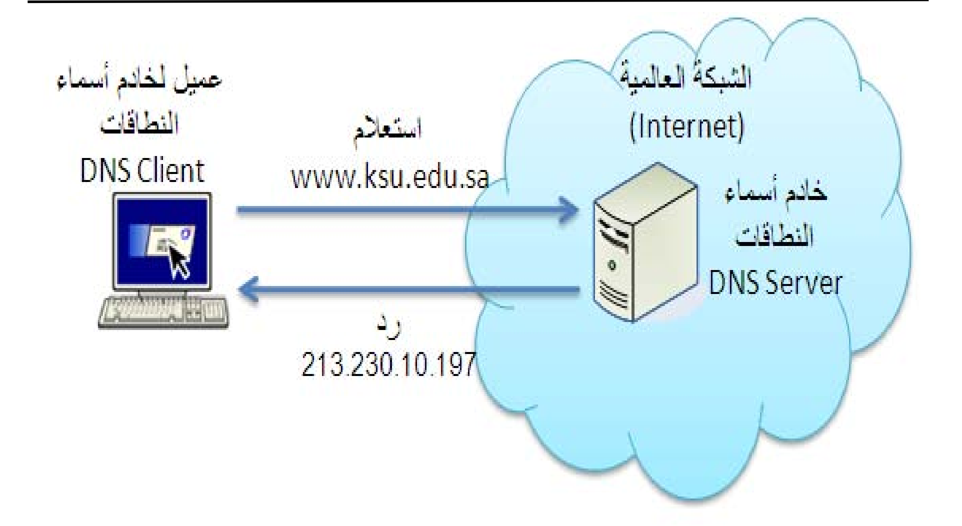
1.4 الأسلوب الأول: تسميم خادم أسماء النطاقات (DNS poisoning)

ويسمى أيضاً (Pharming) أي الزرعة الخبيثة. طريقة هذا الأسلوب أن يقوم المخرب (hacker) بالهجوم على خادم أسماء النطاقات (Domain Name Server – DNS) ، والتلاعب بالسجلات.

كما ذكرنا سابقاً فإن نظام أسماء النطاقات (DNS) هو أحد المكونات الأساسية للشبكة العالمية ، ويتكون من عدة خوادم لأسماء النطاقات تعمل بشكل متكامل. أهم خدمات هذا النظام هو الربط بين أسماء النطاقات وعناوينها العشرية ، لأنه لابد من معرفة العنوان العشري للخادم المراد التخاطب معه ، أي بالإمكان اعتباره دليل الهاتف بالنسبة للشبكة العالمية. فعلى سبيل المثال ، كما في الشكل (4-1) اسم نطاق جامعة الملك سعود (www.ksu.edu.sa) العنوان العشري المسجل لها هو (213.230.10.197)، وبيانات الربط هذه تكون موجودة ومتاحة للاستعلام في أحد خوادم أسماء النطاقات.

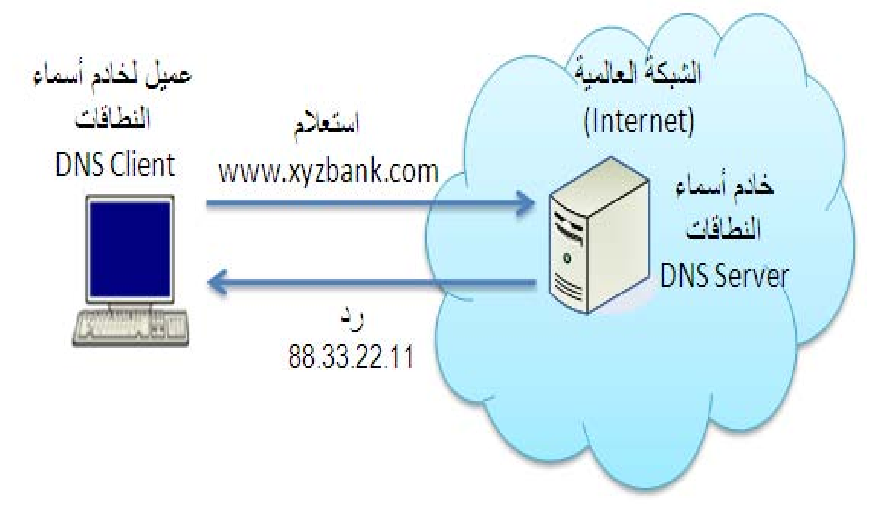
يكون التلاعب بالسجلات بتغيير العناوين العشرية مما يؤدي إلى الإشارة إلى مواقع مزيفة. فكما في مثال جامعة الملك سعود ، فإذا كان خادم الاستعلام مسمماً وتم التلاعب بالسجل الذي يحمل العنوان العشري لجامعة الملك سعود ، فبدلاً من أن يُرجَع خادم أسماء النطاقات العنوان العشري الصحيح لاسم نطاق جامعة الملك سعود ، فإنه سيرجع عنواناً عشرياً مختلفاً يشير إلى موقع مزور.

وكذا الحال كما في مثال جامعة الملك سعود ، فإنه ينطبق على أسماء النطاقات الأخرى ، ومن ضمنها أسماء النطاقات للمصارف وغيرها من المواقع التي تتطلب تزويد بيانات شخصية حساسة وسرية.

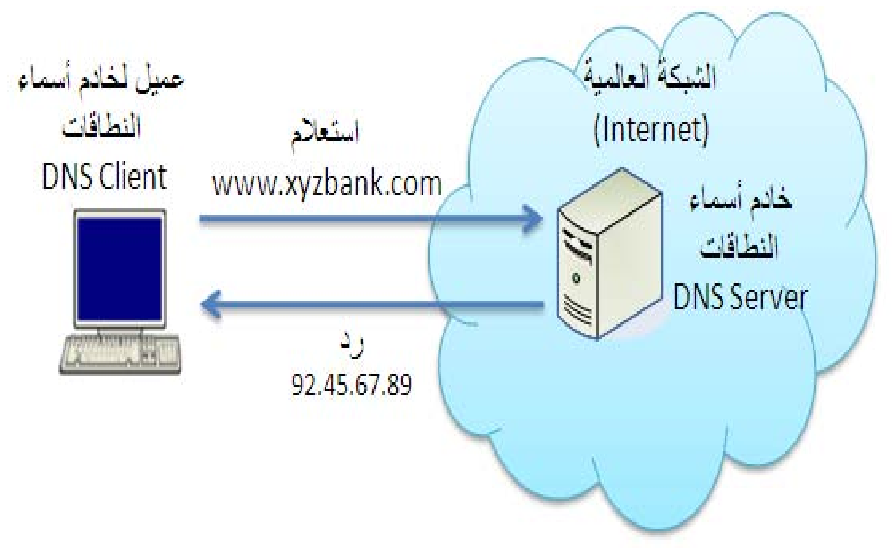


شكل (4-1) استعلام خادم أسماء النطاقات

لنفرض كما في الشكل (4-2) أن اسم النطاق للمصرف "س" هو (xyzbank.com)، وأن العنوان العشري الصحيح للمصرف "س" المقابل لإسم النطاق (xyzbank.com) هو (88.33.22.11)، فعند كتابة شخص ما اسم النطاق لذلك المصرف في متصفح الشبكة العالمية (Internet Browser) سيقوم جهاز الشخص – العميل– ممثلاً ببرنامج المتصفح بالإستعلام عن العنوان العشري للمصرف "س" بإرسال طلب الاستعلام إلى خادم أسماء النطاقات. فإذا صادف وكان ذلك الخادم مسمماً كما في الشكل (4-3) فإنه سيرد بعنوان عشري مزور، وليكن (92.45.67.89) الذي يشير إلى موقع مزيف مستنسخ من الموقع الأصلي للمصرف "س" ، الذي لن يشعر به الضحية أبداً، كون أن اسم نطاق المصرف هو الذي كتبه بنفسه ومتأكد منه، وليس كما رأينا في الأمثلة السابقة من التلاعب في العنوان من حيث جعله مشابهاً إلى حد كبير بالعنوان الصحيح.



شكل (4–2) استعلام خادم أسماء النطاقات



شكل (4–3) استعلام خادم أسماء النطاقات في حالة التسميم

2.4 الأسلوب الثاني: تسميم ملف الخوادم المضيفة (Hosts File Poisoning)

يشبه هذا الأسلوب من أساليب الاصطياد الالكتروني -إلى حد ما- أسلوب تسميم خادم أسماء النطاقات. في هذا الأسلوب يقوم المخربون (hackers) بتسميم ملف الخوادم المضيفة (hosts file) الموجود في جهاز الضحية.

يربط ملف الخوادم المضيفة بين أسماء النطاقات وعناوينها العشرية بصفته خادم أسماء النطاقات ؛ إلا أن ملف الخوادم المضيفة يمكن التحكم به محلياً (locally) من قبل جهاز المستخدم.

عند طلب موقع ما ، فإن جهاز العميل يقوم أولاً بالبحث عن العنوان العشري لاسم الخادم في ملفات الخوادم قبل الاستعلام عن العنوان العشري من خادم أسماء النطاقات.

يعرض الشكل (4-4) السجل الابتدائي في ملف الخوادم المضيفة في نظام التشغيل مايكروسوفت ويندوز (Microsoft Windows).

كما ذكرنا في أسلوب تسميم خادم أسماء النطاقات فإن سجلات الربط بين أسماء النطاقات وعناوينها العشرية يتم تغييرها من قِبَل المخرِّبين لتوجيه الضحايا إلى مواقع مزيفة ؛ والحال نفسه أيضاً في أسلوب تسميم ملف الخوادم المضيفة حيث يقوم المخربون بالشيء نفسه بتسميم ملف الخوادم المضيفة في جهاز الضحية ، وذلك بوضع سجل جديد لربط اسم نطاق معين بعنوان عشري لموقع مزيف.

يعرض الشكل (4-5) السجل المضاف من قِبَل المخرِّب ليتم توجيه الضحية إلى الموقع المزيف (92.45.67.89) بدلاً من الموقع الأصلي والذي افترضنا أن عنوانه (88.33.22.11).

localhost 127.0.0.1

شكل (4-4) ملف الخوادم المضيفة

xyzbank.com 92.45.67.89

شكل (4-5) ملف الخوادم المضيفة بعد العبث به

3.4 الأسلوب الثالث: الاصطياد الالكتروني بواسطة حقن المحتوى (Content Injection)

في هذا الأسلوب يقوم الصيادون بإضافة محتوى خبيث (malicious content) أو حقنةفي موقع صحيح (legitimate site). يمكن أن يقوم هذا المحتوى الخبيث بالتالي:

- إعادة توجيه زائر الموقع الصحيح إلى مواقع أخرى.
- تركيب برامج خبيثة (malware) في جهاز زائر الموقع.
- إعادة توجيه البيانات المدخلة في الموقع إلى خادم الاصطياد الالكتروني.

هناك ثلاثة أنواع أساسية للاصطياد بواسطة حقن المحتوى:

- استغلال ثغرة أمنية في خادم الشبكة العالمية، فيقوم المخرِّبون (hackers) باستبدال المحتوى الأصلي (legitimate content) بمحتوى خبيث (malicious content).
- استغلال ثغرة أمنية في خادم الشبكة العالمية تسمح للمخرِّبين (hackers) حقن أكواد برمجية خبيثة في هذه الخوادم. تعرف هذه الثغرة بـ (Cross-Site Script – XSS)، وهي خلل برمجي (Programming Flaw) يَنتُج من محتوى مضاف من قِبَل

مصدر خارجي. على سبيل المثال، تعليقات الزوار في المدونات (blogs)، أو تقييم الزوار لمنتج ما (user review)، أو رسالة في حلقات النقاش (discussion boards)، أو كلمات بحث في محركات البحث، أو رسالة واردة في البريد الإلكتروني المعتمد على الشبكة العالمية (web-based email).

مثل هذا المحتوى المضاف من قبل مصادر خارجية كما في الأمثلة السابقة قد يكون محتوى على شكل أكواد برمجية خبيثة لم يتم تصفيتها كما هو مفروض من قبل الخوادم المستضيفة لمثل هذه المواقع التي تقبل إضافات من قبل الزوار، مما ينتج عنه عمل هذه الأكواد الخبيثة على متصفح الضحايا عند عرض صفحة الموقع.

من الأمثلة الواقعية على هذا النوع ماورد في أخبار (CNET News.com) 1 عندما قام موقع "PayPal"2 الشهير بالإعلان عن تصحيح ثغرة أمنية في موقعهم الإلكتروني على الشبكة العالمية، وتم حقن موقع خبيث في موقعهم يؤدي إلى إعادة توجيه الضحية عند طلب صفحة إدخال بيانات البطاقة الائتمانية إلى موقع مزيف.

- النوع الثالث من أنواع الاصطياد الالكتروني بواسطة حقن المحتوى هو استغلال ثغرة أمنية في الموقع تسمى ثغرة الحقن عن طريق لغة الاستعلام المركبة (SQL injection vulnerability). في هذه الطريقة يتم تنفيذ أمر في قاعدة البيانات (database command) في الخادم المستضيف للموقع، وقد ينتج عنه تسريب في قاعدة البيانات.

الحقن عن طريق لغة الاستعلام المركبة مثلها مثل حقن الأكواد البرمجية الخبيثة (cross-site script – XSS) هما نتيجة لإهمال تصفيتها كما هو مفروض من قبل

(1) "PayPal fixes phishing hole", by Joris Evers, Staff Writer, CNET News.com, Published: June 16, 2006 4:12 PM PDT, (http://www.news.com/PayPal-fixes-phishing-hole/2100-7349_3-6084974.html).

(2) موقع بيع بالتجزئة على الشبكة العالمية.

الخوادم المستضيفة لمثل هذه المواقع التي تقبل إضافات.

أحد الأمثلة [1] الواقعية لأسلوب الاصطياد الالكتروني بواسطة الحقن عن طريق لغة الاستعلام المركبة (SQL injection vulnerability) هو ماحدث لموقع شركة الأغذية العالمية "كنور" (knorr.com) عندما استطاع أحد زوار الموقع تخطي حاجز تصديق الدخول (login authentication) عن طريق استغلال ثغرة أمنية في الموقع سمحت بالحقن بواسطة لغة الاستعلام المركبة. ببساطة كان استغلال الثغرة الأمنية هذه بإضافة فاصلة منقوطة ";"، والفاصلة المنقوطة في لغة الاستعلام المركبة تترجم إلى أن مايأتي بعدها تعليق لا أهمية له في التنفيذ، فهو مقصود فقط لغرض التوضيح لا أكثر. ويكفي أن يضع المخترق (Hacker) عبارة منطقية صحيحة (true logical expression) قبل الفاصلة المنقوطة في الاستعلام لتكون نتيجة الاستعلام صحيحة، على سبيل المثال وضع العبارة المنطقية (or 'x'='x') في حقل كل من اسم المستخدم وكلمة المرور كفيل في تلك الحالة بتخطي حاجز التصديق.

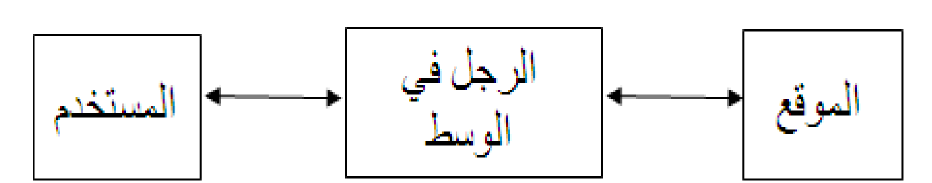
4.4 الأسلوب الرابع: هجمة الرجل في الوسط (Man-in-the-Middle Attack – MITM)

في هذا الأسلوب يقوم الصياد بالتدخل وانتحال شخصية كل من الطرفين خلال عملية الاتصال المباشر على الشبكة العالمية بين المُستخدِم والموقع، كما في الشكل (4-6). الحالة الصحيحة هي أن يتم التراسل بين العميل والخادم مباشرة بدون أي وسيط مجهول لكلا الطرفين، كما في الشكل (4- 7).

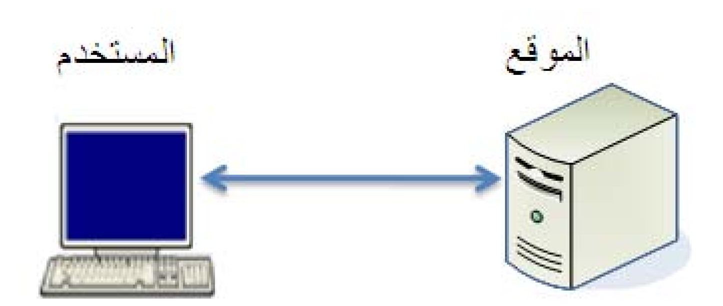
(1) "Knorr.de SQL Injection and XSS Vulnerabilities", Sebastian Bauer, 01/12/07, (http://blog.gjl-network.net/blog/index.php?/archives/78-Knorr.de-SQL-Injection-and-XSS-Vulnerabilities.html)

يتم التدخل من قبل الصياد عن طريق إنشاء اتصال منفصل لكل من المُستخدِم والموقع المراد الاتصال به، و يكون الصياد في المنتصف بين المستخدم والموقع، ما يتيح للصياد استقبال البيانات الصادرة من المستخدم إلى الموقع في عملية الاتصال المباشر (Instant Messaging)، ومن ثم التلاعب بها، وإعادة إرسالها مرة أخرى إلى الموقع الذي ما زال يظن أن البيانات الواردة إليه قادمة من المستخدم. وكما في حالة الإرسال كذلك في حالة الرد فإن الصياد أيضاً يقوم باستقبالها ومن ثم إعادة إرسالها إلى المستخدم كما في الشكل (4-8).

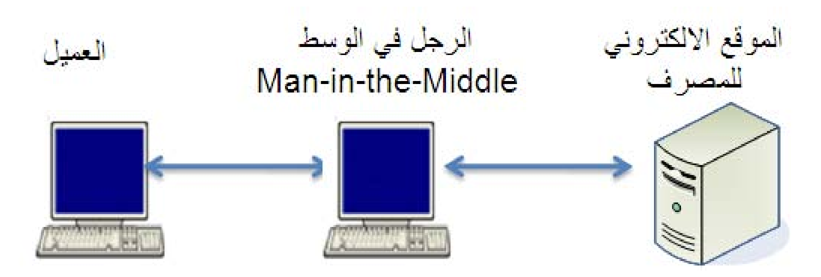
في هذا الأسلوب يظهر أن الاتصال يتم بين طرفين ألا وهما جهاز المستخدم (أو العميل)، وجهاز الموقع (أو الخادم). لكن هم في الحقيقة يتراسلون البيانات عبر جهاز آخر وسيط يعرف بـ "الرجل في الوسط" (Man-in-the-Middle).



شكل(4-6) التراسل في وجود "الرجل في الوسط"



شكل (4-7) التراسل المفترض بين المستخدم والموقع



شكل (4–8) التراسل في حالة وجود الرجل في الوسط

قد تكون فعالية هجمة الرجل في الوسط خلال عملية التراسل بين المُستخدِم والموقع، أو بعد عملية التراسل.

تكون فاعلية الهجمة خلال عملية التراسل، وتسمى بالـ "هجوم النشيط" (Active Attack)، بتغيير المحتوى (content) خلال تدفق البيانات بين المُستخدِم والموقع، فعلى سبيل المثال في حالة التراسل بين مصرف وعميله لغرض التحويل المالي بين الحسابات شكل (4–9) قد يُغيِّر الصياد المخترق (Hacker) رقم الحساب المُراد تحويل الأموال إليه، (مثلا إلى الحساب رقم 4444) بدلاً من الحساب الذي حدده مع العميل، فيقوم المصرف – الذى يتراسل مع الرجل في الوسط – بقبول الطلب وينفذ التحويل المالي إلى الحساب الذي حدده الصياد.

تكون الفاعلية بعد عملية التراسل، وتسمى بالـ "هجوم اللاحق" أو "الهجوم السلبي" (Passive Attack)، بعد تمكن الصياد من التقاط البيانات السرية، كإسم المُستخدِم، ورمز التعريف الشخصي في حال إرسالها من قبل المُستخدِم إلى الموقع، واستخدامها لاحقاً في انتحال شخصية المُستخدِم.



شكل (4–9) تغيير رقم الحساب المحول إليه من قِبَل الرجل في الوسط.

إحدى الطرق لتطبيق "هجمة الرجل في الوسط" هي تسميم خادم أسماء النطاقات (DNS Poisoning) عن طريق التلاعب بالسجلات بتغيير العناوين العشرية كي تشير إلى مواقع مزيفة. مثالاً على ذلك طلب الاستعلام عن العنوان العشري للمصرف "س" فإذا كان خادم الاستعلام مسمماً، وتم التلاعب بالسجل الذي يحمل العنوان العشري لذلك المصرف، فبدلاً من أن يُرجع خادم أسماء النطاقات العنوان العشري الصحيح لاسم نطاق المصرف "س" فإنه سيُرجِع عنواناً عشرياً مختلفاً يشير إلى موقع مزور عن الموقع الأصلي للمصرف "س".

يقع هذا الموقع المزيف تحت سيطرة الصياد تماماً. فعندما يزود عميل المصرف (الضحية) للموقع المزيف باسم المستخدم، ورمز التعريف الشخصي وذلك للدخول إلى حسابه، يتمكن الصياد من معرفة هذه البيانات السرية، ومن ثم يقوم الصياد بالتخاطب مع الموقع الأصلي للمصرف "س" منتحلاً بذلك شخصية العميل الضحية.

5.4 الأسلوب الخامس: تشويش العنوان (Address Obfuscation)

يقوم الصيادون في هذا الأسلوب بتزييف موقع ما، ووضعه تحت اسم نطاق يشبه اسم نطاق الموقع الأصلي.

يعمد الصيادون في هذا الأسلوب إلى أن يكون اسم نطاق الموقع المزيف قريباً

من اسم النطاق الصحيح كي يصعب على الضحية اكتشافه من الوهلة الأولى.

وهناك اختيار آخر لاسم نطاق الموقع المزيف هو أن يكون بمسمى يوحي ويعطي انطباعاً بشرعية الموقع.

مثالاً على اسم نطاق موقع مزيف شبيه باسم نطاق الموقع الأصلي هو مثال مصرف "ساب" السابق ذكره، وقد أضاف الصياد امتداداً بسيطاً لاسم النطاق الصحيح ليصبح (sabb.net.ms)، المشابه لاسم نطاق للموقع الأصلي (sabb.com)، كما في الشكلين (4-10) ، (4-11). ونرى أيضاً أن الموقع المزور صمم ليطابق الموقع الأصلي من حيث النمط، والشعار، والنظر والإحساس.

وأيضا كما في مثال مصرف "سامبا"، السابق ذكره، والموضح في الشكلين (4-12) و(4-13)، اختار الصياد في تلك الحادثة اسماً للموقع المزيف يوحي ويعطي انطباعاً بشرعية الموقع ألا وهو (sambaonlineaccess.com). نجد أنه قد ذكر في اسم النطاق المصرف، وكلمة (onlineaccess) ، وتعني الاتصال المباشر ممايوحي ويعطي انطباعاً بشرعية الموقع، بينما اسم النطاق الصحيح لمصرف "سامبا" هو (sambaonline.com). ونرى أيضا أن الموقع المزور صمم ليطابق الموقع الأصلي من حيث النمط، والشعار، والنظر والإحساس.



شكل (4–10) الموقع المزيف لمصرف "ساب"



شكل(4–11) الموقع الأصلي لمصرف "ساب"



شكل(4–12) الموقع المزيف لمصرف "سامبا"



شكل (4–13) الموقع الأصلي لمصرف "سامبا"

6.4 الأسلوب السادس: الاصطياد الالكتروني عن طريق البرامج الخبيثة (Malware Attack)

تصبح جميع عمليات المستخدم (الضحية) في هذا الأسلوب من خلال متصفح الشبكة العالمية مكشوفة للصيادين. سبب هذا الكشف يعود إلى البرامج الخبيثة (malware) المزروعة في جهاز المستخدم.

تسمح هذه البرامج الخبيثة للصيادبن بمراقبة جميع العمليات المنفذة من خلال متصفح الشبكة العالمية من قبل المستخدم (الضحية). فعلى سبيل المثال عند اتصال المستخدم بالموقع الإلكتروني لمصرف ما، وعند تزويد المستخدم لاسم المستخدم، ورمز التعريف الشخصي للدخول على حسابه المصرفي، ففي حالة وجود مثل هذه البرامج في جهاز الضحية فسيتم إلتقاط هذه البيانات السرية، وإرسالها إلى الصياد الذي سينتحل بدوره شخصية المستخدم في التعامل مع الموقع الإلكتروني للمصرف الذي سيتعامل مع الصياد على أنه العميل الحقيقي.

إحدى الطرق المشهورة لهذا الأسلوب هي تركيب مسجل نقرات لوحة المفاتيح (Keystroke Logger) في جهاز الضحية، والذي من اسمه يقوم بتسجيل النقرات على لوحة المقاتيح، ومن ثم يقوم بإرسالها إلى الصياد، والذي يقوم بدوره بتحليلها، واستخلاص البيانات لانتحال شخصية الضحية.

7.4 الأسلوب السابع: الاصطياد الالكتروني عن طريق محركات البحث (Search Engine Phishing)

توجد طريقة أخرى للاصطياد، وهي إنشاء مواقع إلكترونية للبيع بالتجزئة (Retail) على الشبكة العالمية لمنتجات وهمية. الغرض من هذه المواقع هو خداع

الباحثين عن منتجات معينة على الشبكة العالمية للشراء.

يتم إدخال هذه المواقع للفهرسة في محركات البحث على الشبكة العالمية، ويتم تعبئة مثل هذه المواقع أيضاً بمنتجات مختلفة، وبأسعار منافسة للسوق لجذب الباحثين عن مثل هذه المنتجات.

عندما يبحث شخص ما عن منتج معين عن طريق أحد محركات البحث التي تم فيها فهرسة مواقع بيع بالتجزئة غرضها الاصطياد الالكتروني، فإن ذلك الموقع سيعرض السلعة – نتيجة للبحث– إذا كان يوجد عنده المنتج المطلوب.

عند زيارة المستخدمين هذه المواقع لشراء منتج معين فإنه لغرض إتمام عملية الشراء يطلب منه تعبئة نموذج إلكتروني ببيانات سرية، وذلك إما لإنشاء حساب في ذلك الموقع، أو للتحويل المالي، فيقع المشتري ضحية لذلك الموقع بإفشائه بياناته السرية التي قد تستخدم لاحقاً في انتحال شخصيته.

8.4 الأسلوب الثامن: الاصطياد الالكتروني عن طريق النوافذ المنبثقة (The Popup Attack)

يعد هذا الأسلوب من الأساليب النادرة الحدوث، نظراً لوجود موانع النوافذ المنبثقة (Popup Blocker) بشكل أساسي في معظم متصفحات الشبكة العالمية، ولذا فقد قلّت معدلات نجاح هذا الأسلوب في الآونة الأخيرة. إلا أن هذا الأسلوب كان فعالاً، إلى حد ما، قبل وجود مثل هذه الموانع في المتصفحات.

الطريقة التقليدية لهذا الأسلوب، كما في الشكل (4-14)، هي نافذة مصغرة تنبثق أمام نافذة مكبرة لموقع صحيح، كموقع لمصرف. وفي هذه النافذة المنبثقة يوجد نموذج يطلب من المُستخدِم، تعبئته ببيانات سرية كاسم المُستخدِم،

وكلمة المرور، وذلك كالتحقق من العنوان البريدي، أو غير ذلك من الأسباب، مما يُعطي سبباً منطقياً للمستخدم لتعبئة النموذج.

الهدف الحقيقي من النافذة المكبرة خلف النافذة المنبثقة هو إعطاء المُستخدِم، أو عميل المصرف الضحية شعوراً بشرعية الطلب، وذلك في حال صادف كونه عميلاً لذلك المصرف.



شكل (4–14) النافذة المنبثقة

9.4 الأسلوب التاسع: شريط العنوان المزيف (Fake Address Bar)

يُعَد هذا الأسلوب من أخطر أساليب الاصطياد الالكتروني، ويتم من خلاله استبدال شريط مزيف بشريط العنوان في الجزء الأعلى من نافذة متصفح الشبكة العالمية (web browser) . يمكن هذا الأسلوب الصياد من عرض صفحة إلكترونية مزيفة بالكامل، بينما تبدو لزائر الصفحة على أنها صحيحة.

يتم تنفيذ هذا الأســلوب بإستخدام تقنيات مختلفة مثل "جافا سكربت" (Java Script)، و "جافا أبليت" (Java Applet).

يمكن إخفاء شريط العنوان في متصفح الشبكة العالمية، بإعدادات محددة من قبل صفحة الموقع الإلكتروني، ويتم ذلك بإضافة رموز "جافا سكربت" لهذا الغرض، وتحديداً استخدام الوظيفة (function) "window.open"، وتحديد العنصر "location" بالقيمة "no".

يطبق هذا الأسلوب عند تحويل المستخدم -على سبيل المثال-، عن طريق رابط في رسالة بريد إلكتروني – إلى الموقع المزيف، ويتعرف الموقع على نوع المتصفح المُستخدَم من قِبَل الزائر مباشرة، ومن ثم إخفاء شريط العنوان الحقيقي في المتصفح واستبدال آخر مزيف به، وذلك باستخدام -كما ذكرنا- تقنيات مختلفة مثل "جافا سكربت" (Java Script) أو "جافا أبليت" (Java Applet)، أو حتى يمكن وضع صورة (image) لخداع الزائر بوجود شريط العنوان.

يوضح الشكل (4- 15) شريط عنوان مزيف على هيئة صورة رُكِّب في أعلى الصفحة من متصفح الشبكة العالمية "إنترنت إكسبلورر" [1] (Internet Explorer) لتبدو كأنها حقيقية، ويشير العنوان (www.nike.com/main.html) إلى موقع مختلف

---

1 http://www.microsoft.com/ie

عن الصفحة المعروضة (www.contentverification.com/graphic-attacks/demo/adbarframeset.html).

يعرض الشكل (4-16) المثال السابق نفسه، ولكن باستخدام متصفح آخر للشبكة العالمية "أوبرا" 1 (Opera)، النسخة رقم 9.23، حيث تنكشف خدعة تزييف العنوان بسبب الخاصية الموجودة في المتصفح أوبرا، وهي عرض العنوان الحقيقي للموقع في حال إخفاء شريط العنوان من قبل الصفحة المعروضة. وأيضاً في الشكل نفسه عرض خصائص شريط العنوان المزيف، ونرى أن شريط العنوان المزيف هو صورة (image) بالامتداد (gif).



شكل (4-15) شريط عنوان مزيف على هيئة صورة

(1) opera.com.



شكل (4–16) شريط العنوان المزيف في المتصفح "أوبرا"

مثال آخر على أسلوب شريط العنوان المزيف هو ماحدث 1 لمصرف "سيتي بنك" 2 (Citibank) الأمريكي، عندما أرسلت رسالة بريد إلكترونية منتحلة شخصية المصرف كما في الشكل (4–17)، وكان عنوان المُرسِل هو support@citibank.com والعنوان: "تحقق من بريدك الإلكتروني مع سيتي بنك"، و

(1) http://www.antiphishing.org/phishing_archive/Citibank_3-31-04.htm
(2) www.citibank.com

الفئة المستهدفة من قبل هذا البريد هم عملاء مصرف : "سيتي بنك". يطلب هذا البريد من مُستقبِله الضغط على الرابط الموجود بالرسالة لإكمال عملية التحقق من عنوان بريده الإلكتروني. عند تتبع الرابط يظهر للزائر نموذج يطلب منه رقم بطاقة الصراف الآلي (ATM/Debit card number) ورمز التعريف الشخصي (PIN – Personal Identification Number)، وادعت تلك الرسالة أن الغرض من عملية التحقق هذه هو أن بعض العملاء لم يتصلوا بعناوينهم البريدية، وأنه من أجل ذلك لابد من التحقق!!، الشكل (4-18) يعرض صورة للموقع المزيف لمصرف "سيتي بنك".

كما ذكرنا سابقاً إن عنوان المُرسِل في رسالة البريد الإلكتروني لايعكس بالضرورة شخصية المُرسِل، كما في حالة المثال السابق، حيث يمكن التلاعب بحقل المُرسِل (From)، ووضع أي قيمة فيه.

يعرض الشكل (4-19) صورة الموقع الصحيح لمصرف "سيتي بنك".

احتوت الرسالة في المثال السابق على رابط ظاهره يدل على شرعية الطلب (https://web.da-us.citibank.com/signin/citifi/scripts/E-Mail_verify.jsp) لاحتوائها الرابط على الكلمة "citibank" وهي اسم المصرف، لكنها في الحقيقة تشير إلى الموقع المزيف (http://69.56.202.82/~citisecu/scripts/E-Mail_verify.htm)، كون أن لغة الترميز النصي المتشعب (Hypertext Markup Language – HTML) يتاح من خلالها عرض الرابط بنص مختلف عن العنوان، وقد تم استغلال هذه الثغرة من قبل الصيادين في خداع الضحايا.

From: support@citibank.com
To:
Subject: Verify your E-mail with Citibank
Date: Wed, 31 Mar 2004 10:12:49 -0800

Dear Citibank Member,

This email was sent by the Citibank server to verify your E-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM.

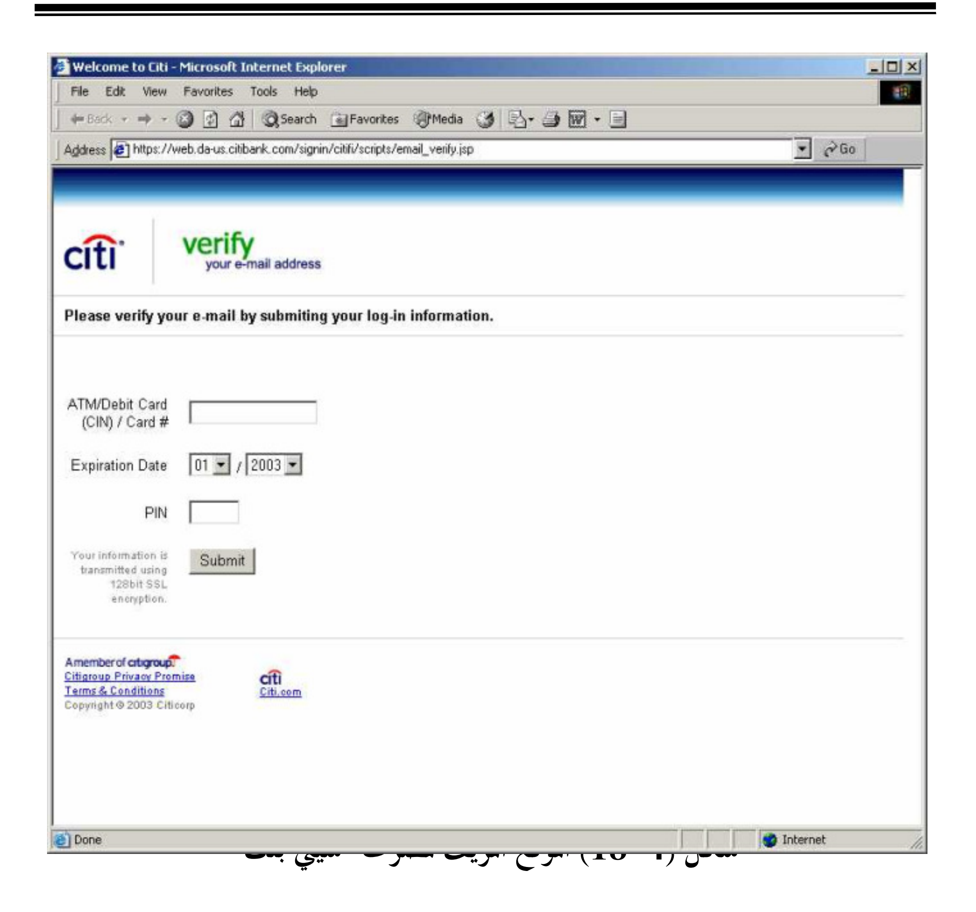
This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it.

To verify your E-mail address and access your bank account, click on the link below:
https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

----

Thank you for using Citibank

اشكل(4–17) نسخة من رسالة البريد الإلكتروني المنتحلة لشخصية مصرف "سيتي بنك"

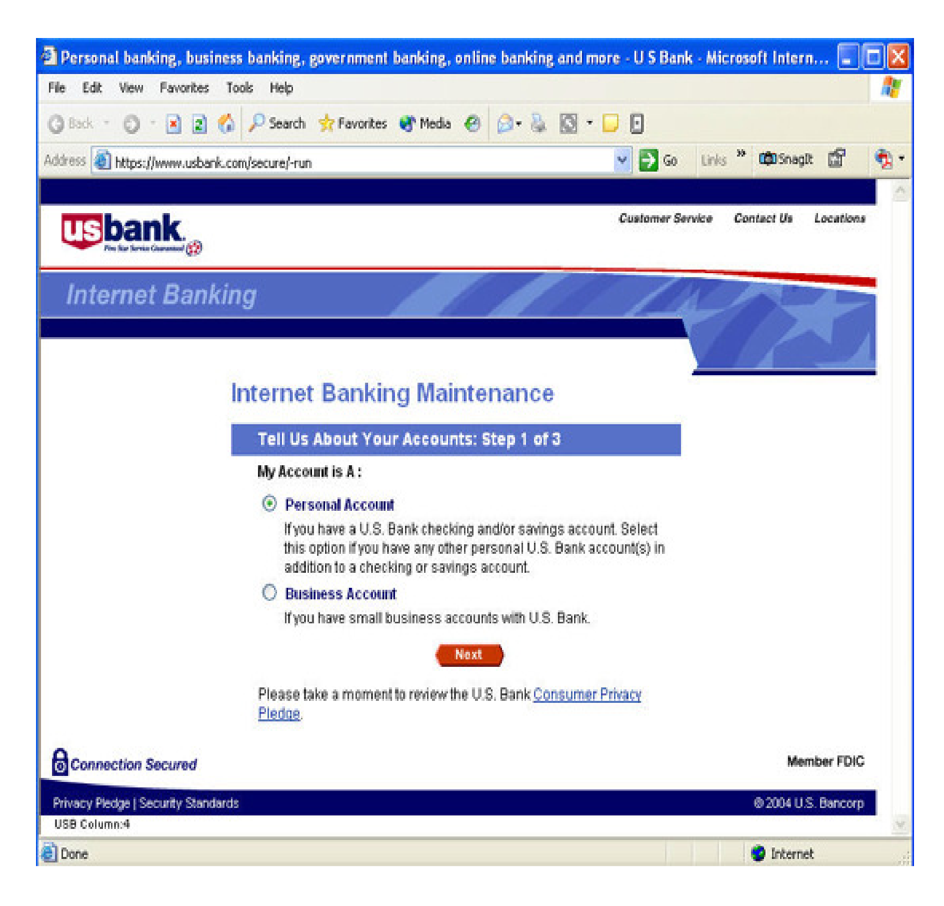


شكل (4-18) الموقع المزيف لمصرف سيتي بنك

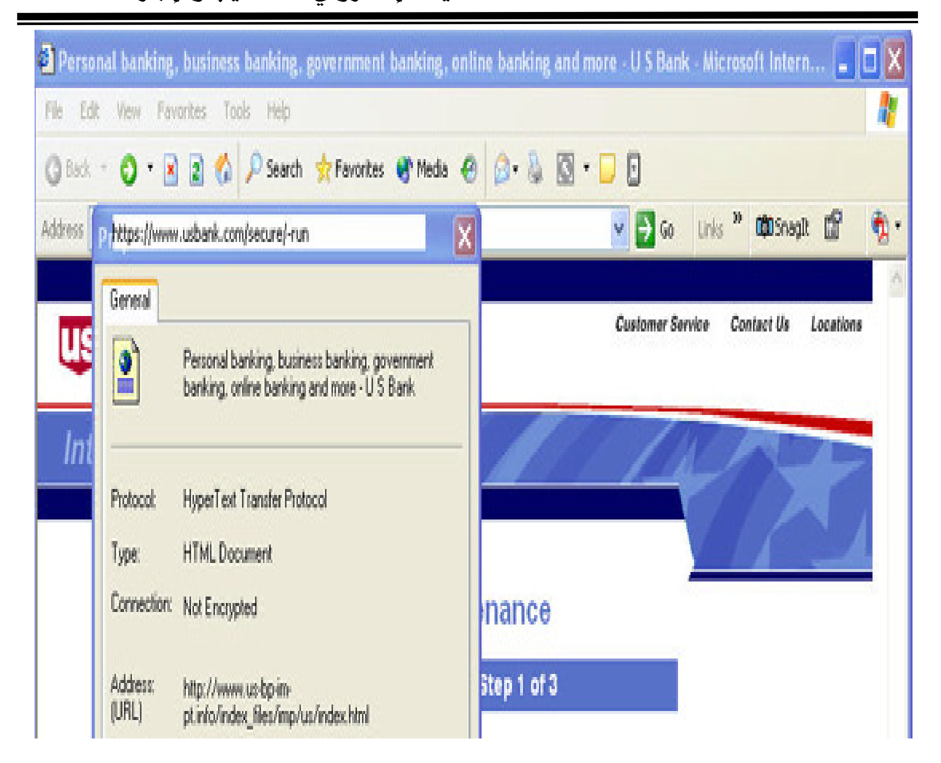
أسلوب آخر [1] لشريط العنوان المزيف يسمى "الشريط النصي الحائم" (hovering text box) وهو وضع حقل نصي (Text Field) بخلفية بيضاء في مكان شريط العنوان الحقيقي في المتصفح، كما في الشكل (4-19) ويصعب اكتشافها من الوهلة الأولى.

(1) http://www.fraudwatchinternational.com/phishing-fraud/phishing-web-site-methods/

يعطي الشكل (4-20) نظرة مُقرَّبة، وذلك عند عرض خصائص الصفحة حيث يعرض عنوان الصفحة الحقيقي، وعند تحريك نافذة الخصائص إلى شريط العنوان يظهر الحقل النصي بوضوح.



شكل (4-19) شريط عنوان مزيف على هيئة حقل نصي



شكل (4–20) نافذة الخصائص توضح حقل النصي

الفصل الخامس
الإجراءات المضادة للاصطياد الإلكتروني
(Phishing Countermeasures)

- **منع هجمات الاصطياد الالكتروني قبل حدوثها**
- **التصفية (Filteration)**
- **التحديثات الأمنية (Security Patches) و جدران الحماية (Firewall)**
- **تصفية الأكواد البرمجية الخبيثة (Cross-Site Script - XSS)**
- **لوحة المفاتيح المرئية (Visual Keyboard)**
- **التصديق الثنائي (Two-Factor Authentication)**
- **التصديق المتبادل (Mutual Authentication)**
- **أشرطة أدوات مكافحة الاصطياد الالكتروني (Anti-Phishing (Toolbars**
- **برامج مكافحة الاصطياد الالكتروني (Anti-Phishing Softwares)**

يناقش هذا الفصل مختلف الإجراءات المضادة لهجمات الاصطياد الإلكتروني.

1,5 الإجراء المضاد الأول: منع هجمات الاصطياد الالكتروني قبل حدوثها[1]

بإمكان المنظمات المحتمل استهدافها من قبل هجمات الاصطياد الالكتروني اتخاذ إجراءات من شأنها تحسين مقاومة هذه المنظمات لهجمات الاصطياد الالكتروني قبل وقوعها، وتقليل الخسائر التي قد تنتج من هجمات الاصطياد الالكتروني.

وتشمل هذه الإجراءات التالي:

1.1.5 إنشاء حساب بريد إلكتروني للبلاغات

تزويد عملاء المنظمة بعنوان بريد إلكتروني ليتسنى لهم الإبلاغ عن الرسائل المنتحلة لشخصية المنظمة. يسمح هذا الحساب بتقرير ما إذا كانت هذه الرسائل صحيحة أم لا، ويعطي أيضاً إنذاراً عن هجمات اصطياد جارية.

2.1.5 مراقبة رسائل البريد الإلكتروني المرتدة (Bounced E-Mails)

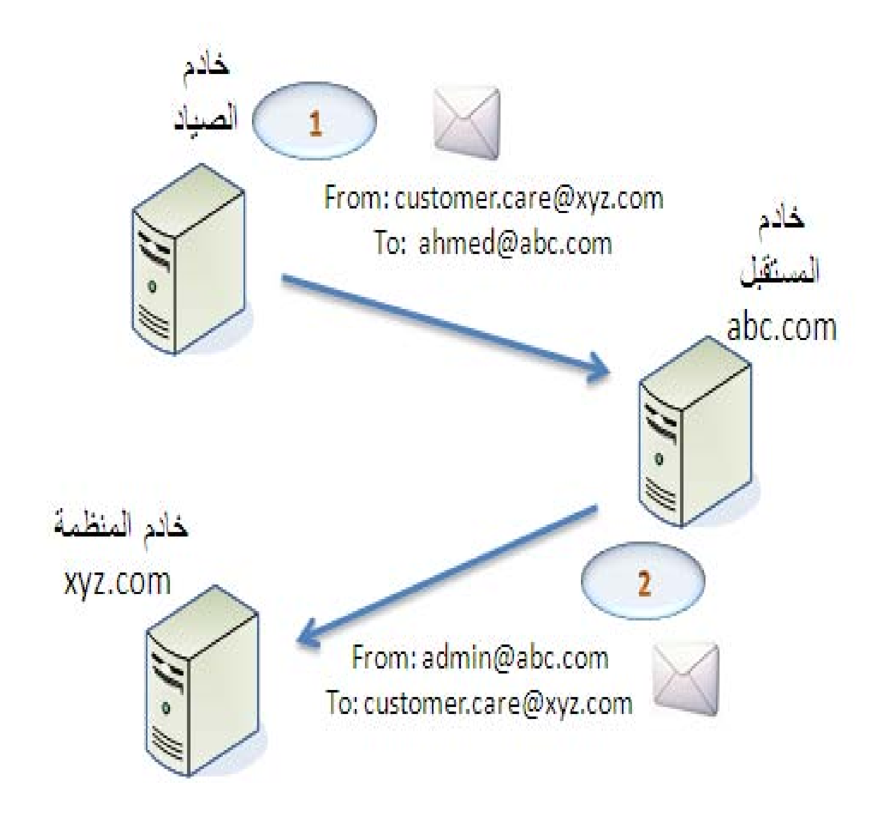
قد تحتوي رسائل الاصطياد الالكتروني المنتحلة لشخصية منظمة ما على عناوين بريد إلكترونية مفبركة غير موجودة في الواقع. عندما يتحقق خادم المُستقبل من هذه العناوين يجد أنها غير مسجلة لديه، فيرجعها إلى الخادم المُرسِل مع إشعار بأن هذه الرسالة لم تصل إلى المُستقبِل لأنه غير مسجل لديه.

بما أن الرسائل أُرسلَت منتحلة شخصية منظمة ما فإن الرسائل المرتدة ستصل إلى خادم المنظمة المنتحل شخصيتها. كثرة الرسائل البريدية المرتدة تشير إلى عمليات اصطياد جارية.

يوضح الشكل (5-1) البريد المرتد (bouncing email)، في الخطوة رقم 1 يقوم خادم المُستقبِل باستلام البريد الإلكتروني المُرسَل من قِبَل الصياد المنتحل

(1) A. Emigh, "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures", Radix Labs, October 3, 2005.

لشخصية المنظمة "xyz.com" حيث وضع الصياد اسم النطاق للمنظمة في الرسالة. بعدما يقوم خادم المُستقبِل بالتحقق من اسم المُستخدِم "ahmed"، يجد أنه غير مسجل لديه في النظام، فيقوم كما في الخطوة رقم 2 بإرجاع الرسالة إلى المُرسِل، أي إلى العنوان الموجود في الحقل (From) من الرسالة.



شكل (5-1) البريد الإلكتروني المرتد (Bouncing Email)

3.1.5 مراقبة مراكز خدمة العملاء

مراقبة كمية الاتصالات وطبيعة الاستفسارات الواردة إلى مراكز خدمة

العملاء. فبعض الأنواع المحددة من الاستفسارات مثل رفض الدخول عبر الموقع الإلكتروني قد توحي بوجود هجمات اصطياد.

4.1.5 مراقبة حسابات العملاء

مراقبة مختلف العمليات على الحسابات، كعدد غير متوقع من محاولات الدخول إلى الحسابات، أو تغيير رمز التعريف الشخصي، أو التحويلات أو السحوبات في حالة المصارف المالية.

5.1.5 مراقبة استخدام الصور المحتوية على شعار المنظمة أو رمزها

يعيد الصيادون أحياناً استخدام ملفات صور الشعارات والرموز المستضافة من قبل المنظمة المستهدفة في مواقعهم المزيفة، بدلاً من استخدام ملفات صور محلية في خوادمهم، أو في الخوادم المستضيفة لصفحاتهم المزيفة.

يمكن اكتشاف مثل هذه الحالات من قبل خادم الشبكة العالمية المستضيف للموقع الإلكتروني للمنظمة، والمستضيف بالتالي لملفات صور رمز المنظمة وشعارها عن طريق التحقق من حقل "المؤشر" (referrer) القادم مع طلب بروتوكول النقل النصي المتشعب (HTTP – Hypertext Transfer Protocol) لتحميل ملف الصورة، الذي سيكون عنوان الصفحة الإلكترونية التي ستعرض الصورة. إذا كان حقل "المؤشر" يشير إلى غير عنوان المنظمة، أو إلى عنوان مجهول فإن الخادم يرفض طلب HTTP لتحميل ملف الصورة، أو قد يعرض الخادم —ما يُعَد حلاً آخر– صورة تحذيرية للتنبيه، بدلاً من الصورة المطلوبة.

هذا الإجراء فعَّال إلى حد ما. فحسب وثيقة طلب التعليقات 1 لبروتوكول النقل النصي المتشعب (HTTP)، فإن حقل "المؤشر" (referrer) وضع لفائدة الخادم،

(1) النسخة الإلكترونية من الوثيقة (http://tools.ietf.org/html/rfc2616).

وأنه حقل اختياري. معنى ذلك الكلام أن بإمكان العميل تغيير قيمة ذلك الحقل، وبالتالي إمكانية التحايل. فبدلاً من أن تشير إلى الصفحة الحقيقية قد توضع فيها أي قيمة، أو تترك فارغة (blank).

إمكانية التحايل في حقل "المؤشر" لاتمنع الاستفادة من التحقق من قيمة ذلك الحقل ما بعد إجراء مضاداً للتصدي لهجمات الاصطياد الالكتروني. فبعض الصيادين قد يكون مبتدئاً في عالم الاصطياد الالكتروني، وجاهلاً في الجوانب الفنية، فلا يلتفت لمثل هذا الاحتيال، فيكون التحقق من حقل "المؤشر" مجدياً في مثل هذه الحالات.

هناك اقتراحات أخرى للاستفادة القصوى من التحقق من قيمة حقل "المؤشر" بوصفه إجراءً مضاداً للتصدي لهجمات الاصطياد الالكتروني، كالتحقق أيضاً من أنه قد تم طلب ملف معين من قبل ذلك العميل، بالإضافة إلى ملف الصورة لضمان أن طلب تحميل ملف الصورة قادم من صفحة موثوقة، ذلك الملف المعين يكون معلوماً فقط لدى الصفحات الموثوقة لتحميل ملفات صور شعار المنظمة ورمزها. وبهذه الطريقة حتى وإن تم التحايل في حقل "المؤشر" من قبل الصيادين فإن بإمكان الخادم التأكد من مصدر طلب ملف الصورة عن طريق التحقق الإضافي وما إذا قد تم طلب ذلك الملف المعين من المصدر طالب ملف الصورة نفسه أم لا؟ إذا كانت النتيجة "لا" فإن الخادم يرفض طلب تحميل ملف الصورة، أو كما ذكرنا يرد الخادم لطالب ملف الصورة بصورة تنبيهية للتحذير من الوقوع في فخ ذلك الصياد.

مثال [1] لتوضيح هذا الإجراء المُضاد، أي"مراقبة استخدام الصور المحتوية شعار المنظمة أو رمزها"، هو ماحدث لمصرف "تشيس" [2]، عندما قام أحد

(1) F-Secure (http://www.f-secure.com/weblog/archives/archive-042006.html)
(2) http://www.chase.com/

الصيادين بإنشاء موقع مزيف وأعاد استخدام صورة شعار المصرف الأصلية المستضافة من قبل خادم المصرف كما في الشكل(5-2).

يعرض الشكل (5-5) يعرض صورة للموقع الحقيقي للمصرف "تشيس" والشكل (5-3) يعرض صورة لشعار مصرف "تشيس".

تطبيق الإجراء المُضاد "مراقبة استخدام الصور المحتوية شعار المنظمة أو رمزها" كان ليحمي ذلك المصرف من هجمة الاصطياد الالكتروني تلك. فالتحقق من مصادر طلب تحميل ملف صورة شعار المصرف كان ليكشف عملية الاصطياد الالكتروني ويمكّن المصرف من إفشالها بالرد بصورة تنبيهية للتحذير كما في الشكل (5-4) بدلاً من الرد بملف شعار المنظمة وذلك لتنبيه الزائر الضحية قبل أن يقع في فخ الاصطياد الالكتروني.

محتوى رسالة التنبيه التحذيرية التي وردت في الشكل (5-4) في هذا المثال هو "إذا رأيت هذه الرسالة، فلا تكتب رقمك السري اتصل بـ..."، وتم وضع رقم للاتصال.



شكل (5–2) الموقع المزيف لمصرف "تشيس"



شكل (5–3) شعار مصرف "تشيس"



شكل (5–4) رسالة التنبيه التحذيرية



شكل (5–5) موقع مصرف "تشيس"

2.5 الإجراء المضاد الثاني: التصفية (Filteration)

تُعَـد تصـفية رسـائل البريـد الإلكترونـي الـتي سـبق شـرحها في الفصـل الثـاني بصـفتها إجـراء مضـاداً للرسـائل غـير المرغوبـة (Spam) أيضـاً فعالـة في كونهـا مضـاداً لهجمـات الاصـطياد الالكترونـي المعتمـدة علـى رسـائل البريـد الإلكترونـي في الخـداع (deception-based phishing emils).

3.5 الإجراء المضاد الثالث: التحديثات الأمنية (Security Patches) وجدران الحماية (Firewalls)

أحد أنواع هجمات الاصطياد الالكتروني هو النوع المعتمد على التقنيات الفنية (technical subterfuge)، ويتم من خلاله استغلال الثغرات الأمنية في جهاز الضحية لزرع برامج التجسس (Spyware)، وتركيب البرامج الخبيثة (malware).

يُعَد تركيب آخر التحديثات الأمنية لأنظمة التشغيل (operating systems)، ومتصفحات الشبكة العالمية (Internet Browsers)، وحماية الأجهزة خلف جدران الحماية إجراءً مضاداً فعّالاً لهجمات الاصطياد الالكتروني المعتمدة على استغلال الثغرات الأمنية.

من الأمثلة [1] على استغلال الثغرات الأمنية في متصفحات الشبكة العالمية عملية اصطياد الثغرة الأمنية في متصفح "موزيلا فايرفوكس" (Mozilla Firefox) النسخة 1.0، التي أتاحت التلاعب وتزييف العنوان (Unified Resource Locator - URL) في نافذة التحميل (download window) التي تنبثق في حال تحميل المستخدم لملف من موقع ما.

هذه الثغرة حدثت بسبب خطأ في تصميم المتصفح، كون نافذة التحميل تعرض العناوين الطويلة بشكل خاطيء. هذه الثغرة قد تُعرِّض المُستخدِمين للخطر. أقرب طريقة لوقوع المستخدمين ضحية نتيجة استغلال هذه الثغرة هي عن طريق الضغط على رابط في رسالة بريد إلكترونية والذي يشير إلى موقع مزيف، ومن ثم تحميل برامج خبيثة من ذلك الموقع المزيف، وبهذا تظهر للمستخدم الضحية على أنها

(1) “Firefox flaw raises phishing fears”, by Ingrid Marson, Published: January 7, 2005 11:06 AM PST , (http://www.news.com/Firefox-flaw-raises-phishing-fears/2100-1002_3-5517149.html)

تحمل من موقع صحيح.

بعد اكتشاف هذه الثغرة أصدرت "موزيلا فايرفوكس" التحديثات اللازمة لِسَد هذه الثغرة، ووجب على جميع مستخدمي المتصفح تحديثه لتفادي خطر الوقوع ضحية لاستغلال هذه الثغرة.

4.5 الإجراء المضاد الرابع: تصفية الأكواد البرمجية الخبيثة (Cross-Site Script - XSS)

كما ذكرنا في أسلوب حقن المحتوى الخبيث (malicious content injection) من أساليب الاصطياد الالكتروني، أن الصيادين يقومون بإضافة أو حقن محتوى خبيث (malicious content) إلى موقع صحيح (legitimate site). يمكن أن يقوم هذا المحتوى الخبيث بالتالي:

- إعادة توجيه زائر الموقع الصحيح إلى مواقع أخرى.
- تركيب برامج خبيثة (malware) في جهاز زائر الموقع.
- إعادة توجيه البيانات المدخلة في الموقع إلى خادم الاصطياد الالكتروني.

يمكن تحقيق ذلك الأسلوب بحقن المحتوى عن طريق استغلال ثغرة أمنية في خادم الشبكة العالمية ما يتيح للمخرِّبيين (hackers) حقن أكواد برمجية خبيثة في هذه الخوادم. تعرف هذه الثغرة بـ (cross-site script - XSS)، وهي خلل برمجي (programming flaw) ينتج من محتوى مضاف من قبل مصدر خارجي. على سبيل المثال تعليقات الزوار في المدونات (blogs)، أو تقييم الزوار لمنتج ما (user review)، أو رسالة في حلقات النقاش (discussion boards)، أو كلمات بحث في محركات البحث، أو رسالة واردة في البريد الإلكتروني المعتمد على الشبكة العالمية

(web-based email).

الطريقة المثلى لتفادي خطر الوقوع ضحية الاصطياد الالكتروني بأسلوب حقن المحتوى الخبيث، هو تصفية هذه الأكواد وإبعادها قبل حفظها في الخادم وبالتالي ضمان عدم عرضها على متصفحات الزوار.

5.5 الإجراء المضاد الخامس: لوحة المفاتيح المرئية (Visual Keyboard)

تعد هذه طريقة بديلة لإدخال البيانات السرية عن الطريقة التقليدية، ويتم إدخالها عن طريق لوحة مفاتيح مرئية في صفحة الدخول الإلكترونية، ويختار المستخدم منها بواسطة تحريك الفأرة والنقر على المفتاح المطلوب من لوحة المفاتيح المرئية على الشاشة.

تطبق لوحة المفاتيح المرئية إجراءً مضاداً لسرقة البيانات السرية عن طريق البرامج الخبيثة (malware) التي تسجل نقرات لوحة المفاتيح (key logging) من جهاز الضحية، ومن ثم تقوم بإرسالها إلى الصياد، الذي يقوم بتحليلها، واستخلاص البيانات لانتحال شخصية الضحية.

يعرض الشكل (5-6) لوحة المفاتيح المرئية لأحد المصارف المستخدمة لإدخال بيانات العميل السرية للدخول إلى حسابه.

لوحة المفاتيح المرئية فعَّالة إلى حد ما، فلم يتسن للصيادين حتى الآن تطوير برامج خبيثة لالتقاط البيانات المطبوعة من لوحة المفاتيح المرئية في ظل قلّة استخدام لوحة المفاتيح المرئية في المواقع الإلكترونية.

قد يتمكن المخرِّبون لاحقاً من تطوير برامج خبيثة للتعرف على البيانات المكتوبة بواسطة لوحة المفاتيح المرئية.



شكل (5–6) لوحة المفاتيح المرئية في صفحة الدخول لأحد المصارف

6.5 الإجراء المضاد السادس: التصديق الثنائي (Two-Factor Authentication)

يعرف أيضاً بـ "التصديق القوي" (Strong Authentication). في هذا الإجراء يتم استخدام طريقتين من طرق التصديق لضمان درجة أعلى من التصديق.

هناك ثلاث طرق للتصديق:

- ماذا تعرف؟ "what you know?" : كاسم المستخدم، وكلمة المرور.
- ماذا تملك؟ "what you have?" : كالبطاقة الذكية (smart card)
- من أنت؟ "what you are?"، : وهي الصفات الحيوية، كبصمة الإصبع (fingerprint).

الطريقة التقليدية المستخدمة في عملية التصديق، هي النوع الأول، ويتم فيها تزويد طالب التصديق ببيانات متوقعة ومعروفة لكل من الطرفين في عملية الاتصال، كاسم المستخدم، وكلمة المرور.

في التصديق الثنائي يتم استخدام نوعين من الأنواع المذكورة أعلاه، كتزويد اسم المستخدم، وكلمة المرور، وبصمة الأصبع، أو استخدام البطاقة الذكية.

مثال على التصديق الثنائي بطاقة الصراف (ATM card)، والتي تستخدم للسحب النقدي من أجهزة الصرف الآلي. في عملية السحب النقدي يقوم العميل بإدخال البطاقة، والتي تعد من النوع الثاني "ماذا تملك؟"، ويقوم أيضاً بإدخال كلمة المرور الذي يعد من النوع الأول "ماذا تعرف؟".

عادة في عمليات الاصطياد الالكتروني تسرق البيانات السرية، مثل كلمة المرور، التي تصنّف من النوع الأول "ماذا تعرف؟"، لذلك يتم طلب بيانات أخرى إضافية في عملية التصديق، كبيانات تنتمي إلى النوعين الآخرين من أنواع التصديق "ماذا تملك؟"، أو "ما أنت؟".

التصديق الثنائي يستخدم إجراءاً مضاداً لهجمات الاصطياد الالكتروني عن طريق هجمة الرجل في الوسط (Man-in-the-middle Attack)، والاصطياد الالكتروني عن طريق تزييف المواقع، وانتحال الشخصية (Identity Attack).

7.5 الإجراء المضاد السابع: التصديق المتبادل (Mutual Authentication)

ويعرف أيضاً بـ "التصديق الثنائي الاتجاه" (Two-way Authentication). في هذا الإجراء يُصدِّق كلٍ من العميل والخادم بعضهما الآخر، فيقوم الخادم بتصديق العميل عن طريق رمز التعريف الشخصي، أو غيره من وسائل التصديق، كالمقاييس الحيوية (Biometrics)، وأيضاً يتم تصديق الخادم من قبل العميل، ويتحقق من أنه متصل بالخادم المقصود، وليس بمنتحل لشخصية الخادم كأن يكون موقعاً مزيفاً.

يتيح التصديق المتبادل لكل من الطرفين في عملية اتصال طرقاً للتحقق من صحة هوية بعضهما ببعض.

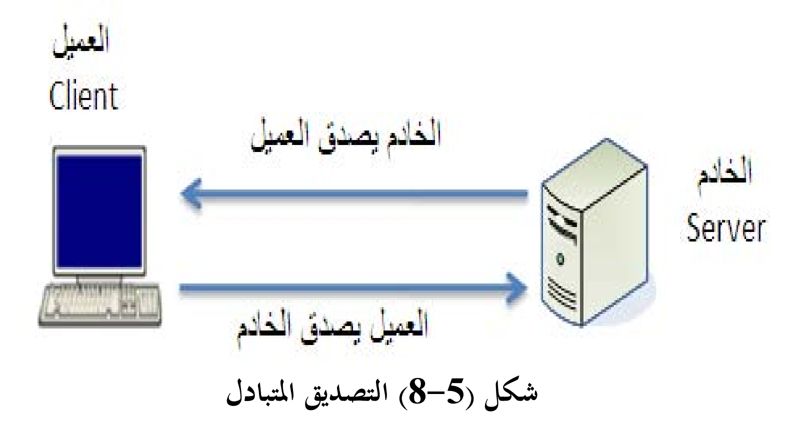
يوضح الشكل (5-7) عملية التصديق الأحادي الاتجاه؛ ويوضح الشكل (5- 8) عملية التصديق المتبادل.

إحدى الطرق المستخدمة لتصديق الخادم من قبل العميل، هي أنه حين يقوم العميل بالتسجيل لدى الخادم فإن العميل يختار صورة أو جملة (phrase) تستخدم لاحقا لتصديق الخادم من قبل العميل. فعند إنشاء اتصال بين العميل والخادم، يقوم الخادم بعرض الصورة والجملة المحددة مسبقاً في عملية التسجيل، فإذا كانت الصورة والجملة صحيحتين يتم تصديق الخادم.

التصديق المتبادل يستخدم إجراءً مضاداً لهجمات الاصطياد الالكتروني عن طريق هجمة الرجل في الوسط (Man-in-the-Middle Attack)، والاصطياد الالكتروني عن طريق تزييف المواقع، وانتحال الشخصية (Identity Attack).



شكل (5-7) التصديق الأحادي الاتجاه



شكل (5-8) التصديق المتبادل

8.5 الإجراء المضاد الثامن: أشـــــــرطة أدوات مكافحـــة الاصـــطياد الالكتروني (Anti-Phishing Toolbars)

شريط الأدوات هو شريط يحوي عدة أزرار لعمل وظائف معينة ؛ ويكون عادة في الجهة العلوية من تطبيق ما (Application). يعرض الشكل (5-9) شريط أدوات "جوجل" على متصفح الشـــبكة العالمية "إنترنت إكســبلورر" (Internet Explorer).

رداً على خطر هجمات الاصطياد الالكتروني قام العديد من الشركات كشركة "eBay" ومنتجي البرمجيات، كـ "مايكروسوفت" بانتاج أشرطة أدوات متخصصة في مكافحة الاصطياد الالكتروني تركب إضافات (Add-on) على متصفحات الشبكة العالمية، وبرامج عميل البريد الإلكتروني (E-Mail Client).

وظيفة هذه الأشرطة بشكل عام هو تنبيه المستخدم عند زيارته مواقع اصطياد مشبوهة. يتاح من خلال أشرطة أدوات مكافحة الاصطياد الالكتروني التعرف على مواقع أو رسائل الاصطياد الالكتروني عن طريق الاستعلام عن الموقع المراد زيارته من قبل المستخدم، أو عن البريد الوارد من قواعد بيانات (databases) تُسجَّل فيها مواقع ورسائل الاصطياد الالكتروني، سواء المكتشفة أو المشبوهة، التي يتم تحديثها من قبل جهات متخصصة في اكتشاف مواقع الاصطياد الالكتروني، أو عن طريق البلاغات الواردة من مستخدمين آخرين. وبعض الأدوات تستخدم طرقاً متقدمة في التعرف على رسائل ومواقع الاصطياد الالكتروني، كتطبيق الطرق ا لتجريبية (heuristic methods) للتعرف على المظاهر (patterns) لاكتشاف عمليات الاصطياد الالكتروني.

يعرض الجدول (5-1) قائمة لمختلف أشرطة أدوات مكافحة الاصطياد الالكتروني، بالإضافة إلى روابطها على الشبكة العالمية.

مثالاً على أشرطة أدوات مكافحة الاصطياد الالكتروني، برنامج (Phishing Filter) [1] المدمج مع المتصفح "إنترنت إكسبلورر" النسخة السابعة. يتحقق هذا البرنامج من كل صفحة يطلب المستخدم زيارتها، إذا كانت الصفحة مشبوهة فسيظهر في أعلى المتصفح -بجانب شريط العنوان- زر باللون الأصفر لتحذير

(1) "Microsoft Phishing Filter: A New Approach to Building Trust in E-Commerce Content", anti-phishing white paper, Microsoft.com,2005

المستخدم، بالضغط على الزر ستعرض رسالة تنبيهية تنصح بعدم إفشاء أي بيانات سرية، أو شخصية لهذه الصفحة، كما في الشكل (5-10).

في حال تأكد برنامج (Phishing Filter) من أن الموقع المطلوب زيارته من قبل المُستخدِم هو موقع اصطياد - سيظهر في أعلى المتصفح – بجانب شريط العنوان – زر باللون الأحمر لتحذير المُستخدِم، بالإضافة أنه سيمنع عرض صفحة الاصطياد الالكتروني، ويعرض بدلاً منها صفحة تحذيرية فيها خياران، إما إغلاق الصفحة، أو الاستمرار في عرض صفحة الاصطياد الالكتروني على مسؤولية المُستخدِم، كما في الشكل (5-11).

مثال آخر هو شريط الأدوات "SpoofGuard" [1] المعروض في الشكل (5-12). تتحقق هذه الأداة من الموقع المراد زيارته من قبل المستخدم، فإذا كان الموقع قد عُرِّف على أنه موقع اصطياد فستعرض الأداة أيقونة حمراء، وإذا لم تستطع الأداة التعرف على ما إذا كان الموقع موقع اصطياد أم لا فستعرض الأداة أيقونة صفراء، وإذا تم التحقق من الموقع على أنه آمن فستعرض الأداة أيقونة خضراء.

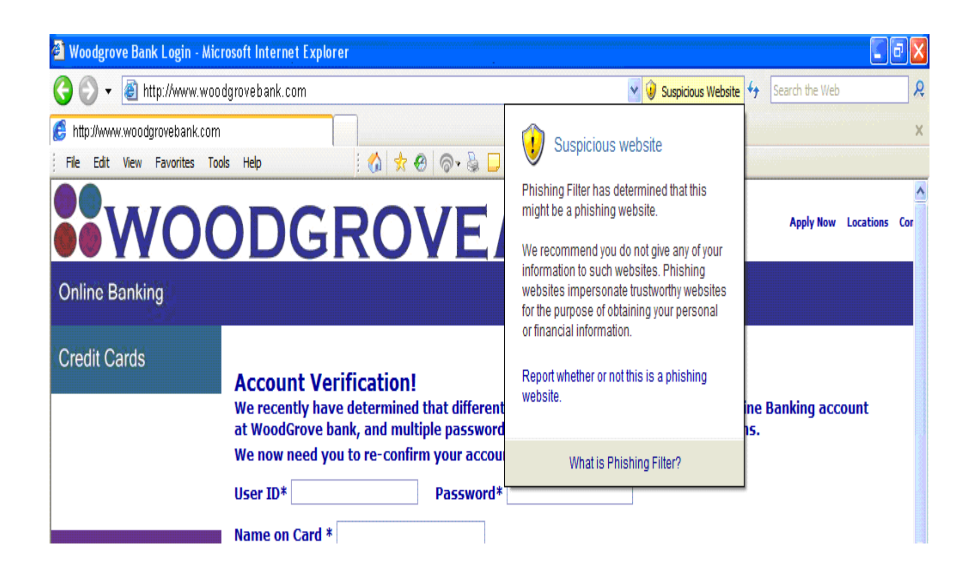


شكل (5-9) شريط أدوات جوجل على متصفح الشبكة العالمية "إنترنت إكسبلورر" (Internet Explorer)

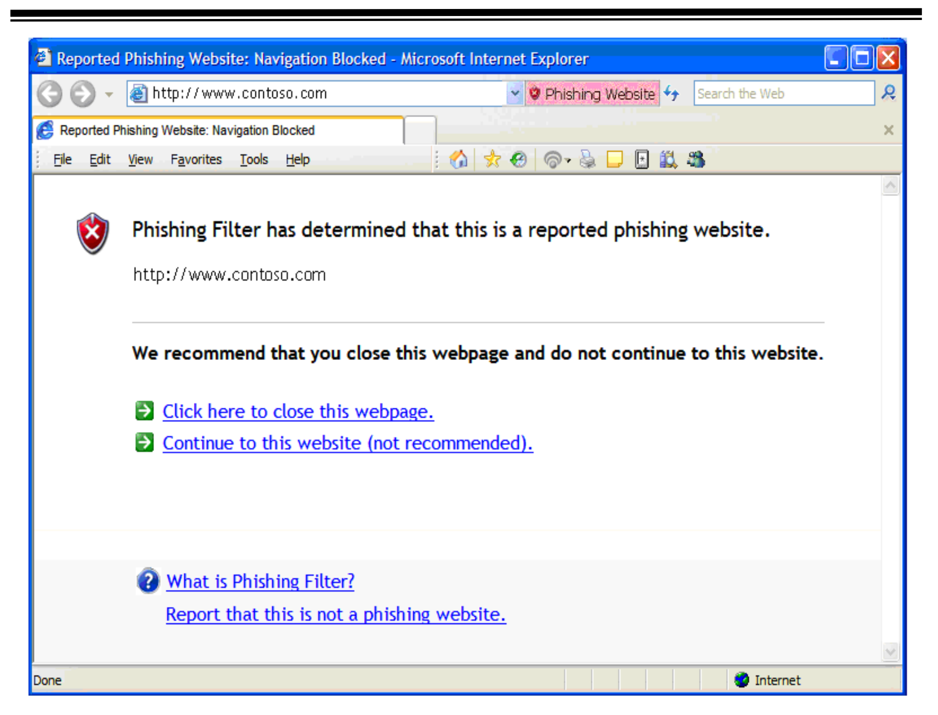
1 crypto.stanford.edu/SpoofGuard/

الجدول (5-1). قائمة أشرطة أدوات مكافحة الاصطياد الالكتروني .

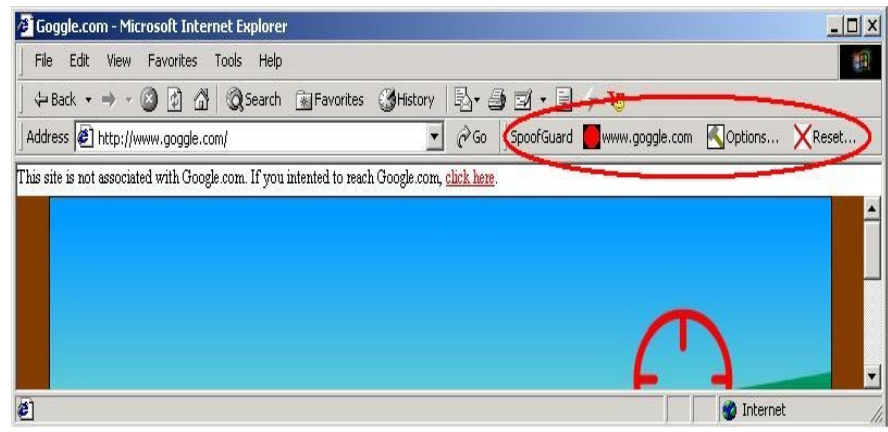
رابط الشبكة العالمية	شريط الأدوات
microsoft.com/ie	Internet Explorer 7 Phishing Filter
pages.ebay.com/ebay_toolbar	eBay
www.callingid.com	CallingID
cloudmark.com	CLOUDMARK
earthlink.net	EarthLink
toolbar.trustwatch.com	TrustWatch
crypto.stanford.edu/SpoofGuard	SpoofGuard



شكل (5-10) رسالة التنبيه عن مواقع الاصطياد الالكتروني المشبوهة في المتصفح "إنترنت إكسبلورر"



شكل (5–11) رسالة التنبيه عن مواقع الاصطياد الالكتروني في المتصفح "انترنت اكسبلورر"



شكل (5–12) شريط أدوات مكافحة الاصطياد الالكتروني "SpoofGuard"

9.5 الإجراء المضاد التاسع: برامج مكافحة الاصطياد الالكتـــروني (Anti-Phishing Software)

تتضـمن معظـم بـرامج الحمايـة (security software) الحمايـة ضـد هجمـات الاصـطياد الالكترونـي بنوعيهـا المعتمـد علـى الرسـائل، أو المعتمـد علـى اسـتغلال الثغرات الأمنية.

تسـتطيع هـذه الـبرامج عمومـاً التعـرف علـى مواقـع ورسـائل الاصـطياد الالكتروني بالطريقة نفسها المتبعة في أشرطة أدوات مكافحة الاصـطياد الالكترونـي، فـبرامج الحمايـة تقـوم بتركيـب أشـرطة أدوات إضـافات علـى متصـفحات الشـبكة العالمية، وبرامج عميل البريد الإلكتروني.

تتـيح الحمايـة حلـولاً متكاملـة. فبالإضـافة إلى التصـدي لهجمـات الاصـطياد الالكترونـي، فإنهـا أيضـاً تكـافح الـبرامج الخبيثـة (maleware)، ومسـجلات نقـرات لوحة المفاتيح (key logger)، التي قد تؤدي إلى سرقة البيانات السرية، والشخصية.

تحديث برامج الحماية المستمر شرط أساسي لتحقيق الفائدة المرجوة منها.

الجـدول (5-2) يعـرض قائمـة لـبرامج الحمايـة المشـتملة علـى الحمايـة ضـد هجمات الاصطياد الالكتروني، بالإضافة إلى روابطها على الشبكة العالمية.

جدول (5-2) قائمة برامج الحماية ضد هجمات الاصطياد الالكتروني

برنامج الحماية	رابط الشبكة العالمية
Kaspersky Internet Security	kaspersky.com
Norton Internet Security	symantec.com
McAfee Internet Security Suite	mcafee.com
Trend Micro Internet Security	trendmicro.com
BitDefender Internet Security	bitdefender.com
AVG Internet Security	grisoft.com
Panda Internet Security	pandasecurity.com

معجم المفردات

Access	اتصال
Active Attack	الهجوم النشيط
Address Obfuscation	تشويش العنوان
ATM	أجهزة الصرف الآلي
Anti-Phishing Toolbars	أشـــــرطة أدوات مكافحــــة الاصــــطياد الالكتروني
Anti-Phishing Softwares	برامج مكافحة الاصطياد الالكتروني
Application	تطبيق
Attachments	مرفقات
Attacker	المهاجم
Authentication	التصديق
Backdoors	أبواب خلفية
Bandwidth	سعة قناة الاتصال
Bank	مصرف
Biometrics	المقاييس الحيوية
Black List	القائمة السوداء
Blog	مدونة
Bounced E-Mail	رسائل البريد الإلكتروني المرتدة
Browser	المتصفح

Chat Rooms	غرف المحادثة
Commercial Whitelists	القوائم البيضاء التجارية
Computer	حاسوب
Configuration	تهيئة / اعداد / ضبط
Content	محتوى
Cracker	مخرّب
Database	قاعدة بيانات
Data Integrity	سلامة (أو تكامل) البيانات
Dialog Box	صندوق حواري
Dictionary Attack	هجمة القاموس
Discussion Boards	حلقات النقاش
DNS Poisoning	تسميم خادم أسماء النطاقات
Domain Name	اسم النطاق
Download	تحميل
E-mail	البريد الإلكتروني
E-mail account	حساب البريد الإلكتروني
E-mail address	عنوان البريد الإلكتروني
E-mail client	برنامج عميل البريد الإلكتروني
E-mail Filtering	تصفية البريد الإلكتروني
E-Mail Header	ترويسة رأس الرسالة
E-Mail Route	مسار رسالة البريد الإلكتروني

E-mail Server	خادم البريد الإلكتروني
Fax	ناسوخ (الفاكس)
Filtering	تصفية
Firewalls	جدار الحماية
Form	نموذج
Forums	المنتديات
Hackers	مخترقو الشبكة العالمية (الهاكرز)
Heuristics Methods	الطرق التجريبية
Hosts File	ملف الخوادم المضيفة
HTML	لغة الترميز النصي المتشعب
HTTP	برتوكول النقل النصي المتشعب
Inquiry	استعلام
Install	تركيب / تنصيب / تثبيت
Instant Messenging	التراسل الآني / التراسل المباشر
Internet	الشبكة العالمية
Integrity Check	التحقق من التكاملية
IP Address	عنوان بروتوكول الانترنت
IPS	أنظمة منع الاختراقات
Junk mail	البريد غير المرغوب
Keystroke Logger	مسجل نقرات لوحة المفاتيح
Locally	محلي

Look and Feel	النظر والإحساس
Malicious content	محتوى خبيث
Malware	البرامج الخبيثة
Man-In-The-Middle	هجمة الرجل في الوسط
Message body	نص الرسالة
Mutual Authentication	التصديق المتبادل
OCR	التعرف على الحوف ضوئياً
Online	اتصال آني / اتصال مباشر
Online trust	الوثوق الآني
Open Mail Rely	خادم البريد الإلكتروني المفتوح
Operating System	نظام التشغيل
Passive Attack	الهجوم اللاحق / الهجوم السلبي
Password	كلمة المرور
Pharming	التلاعب في سجلات خادم أسماء النطاقات / الزرعة الخبيثة
Phishing	الاصطياد الالكتروني
POP3	بروتوكول مكتب البريد
Popup	الصفحات المنبثقة
Programming Flow	خلل برمجي
Regular Expressions	التعبيرات المألوفة
Scam	عمل خدّاع

Search Engines	محركات البحث
Security Updates	التحديثات الأمنية
Server	الخادم
Smart Card	البطاقة الذكية
SMTP	بروتوكول نقل البريد البسيط
SMS	رسالة نصية قصيرة
Social Engineering	الهندسة الاجتماعية
Spywares	برامج التجسس
Strong Authentication	التصديق القوي
Subject	موضوع الرسالة
Text Field	حقل نصّي
Tools	الأدوات المساعدة
Traffic	التدفق
Two-Factor Authentication	التصديق الثنائي
Upgrade	إصدارات الترقية
User name	اسم المستخدم
Version number	رقم النسخة
Virus	فيروس
Visual Keyboard	لوحة المفاتيح المرئية
Vulnerability	ثغرة
Web browser	متصفح الشبكة العالمية

البريد الإلكتروني المبني على الشبكة العالمية	Webmail
القائمة البيضاء	White List
نافذة	Window
دودة	Worm
الشبكة العالمية	www

المراجــــع

- Jonathan B. Postel, "SIMPLE MAIL TRANSFER PROTOCOL", RFC 821, (http://tools.ietf.org/html/rfc821), August 1982.
- Network Working Group, "Requirements for Internet Hosts -- Application and Support", RFC 1123, (http://tools.ietf.org/html/rfc1123), May 1996.
- Network Working Group, "Post Office Protocol - Version 3", RFC 1939, (http://tools.ietf.org/html/rfc1939), May 1996.
- Network Working Group, "MAIL ROUTING AND THE DOMAIN SYSTEM", RFC 974, (http://tools.ietf.org/html/rfc974) , January 1986.
- Network Working Group, "Common DNS Operational and Configuration Errors", RFC 1912, (http://tools.ietf.org/html/rfc1912) , February 1996.
- "تقييم الوضع الراهن للرسائل الاقتحامية في المملكة العربية السعودية"، هيئة الاتصـــالات وتقنيـــة المعلومـــات، 1429هـــ- 2008م، (http://www.spam.gov.sa/Statistics-Arabic.doc)
- The State of Spam, A Monthly Report – February 2007, Generated by Symantec Messaging and Web Security (http://www.symantec.com/avcenter/reference/Symantec_Spam_Report_-_February_2007.pdf).
- 2006 Spam Trends Report: Year of the Zombies, December 27, 2006, Commtouch® Software Ltd., (http://www.commtouch.com/documents/Commtouch_2006_Spam_Trends_Year_of_the_Zombies.pdf).
- CALIFORNIA BUSINESS AND PROFESSIONS CODE, DIVISION 7, PART 3, CHAPTER 1, ARTICLE 1.8.Restrictions On Unsolicited Commercial E-mail Advertisers.
- "Virus description service" from "F-Secure", (http://www.f-secure.com/v-descs/novarg.shtm).
- جريدة الأخبار 24 الجنوب أفريقية بتاريخ 31\ديسيمبر\2004 بعنوان: SA cops, Interpol probe murder" " (http://www.news24.com/News24/South_Africa/News/0,,2-7-1442_1641875,00.html)
- Thomas A. Knox,Technologies to Combat Spam, GIAC Security Essentials

Certification (GSEC) Practical Assignment, Version 1.4b, Option 1 , SANS Institute, June 16, 2003.

- "Gmail uses Google's innovative technology to keep spam out of your inbox", gmail.com, (http://www.google.com/mail/help/fightspam/spamexplained.html), December, 2007.
- " Nick Johnston, PDF Spam: Spam Evolves, PDF becomes the Latest Threat", Anti-Spam Development at MessageLabs, A MessageLabs Whitepaper, August 2007.
- Anti-Spam Research Group (ASRG) of the Internet Research Task Force (IRTF), (http://asrg.sp.am/).
- Mark Ciampa, "Security + Guide to Network Security Fundamentals", 2nd edition, THOMSON, 2005.
- M. Jakobsson, S. Myers, "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft", WILEY, 2007.
- R. Lininger, R. Vines, "Phishing: Cutting the Identity Theft Line", WILEY, 2005.
- L. James, "Phishing Exposed", SYNGRESS, 2005.
- A. Emigh, "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures", Radix Labs, October 3, 2005.
- "وقفة تحليلية لحادثة رسالة الاصطياد الالكتروني الموجهة لعملاء احد البنوك السعودية"، خالد الغثبر، جريدة الرياض السعودية، السبت 14 من ذي الحجة 1426هـ - 14 يناير 2006م - العدد 13718
- Christopher Abad, "The economy of phishing: A survey of the operations of the phishing market", First Monday, volume 10, number 9, September 2005, (http://firstmonday.org/issues/issue10_9/abad/index.html). M. Jakobsson, S. Myers, "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft", Wiley, 2007.
- The Anti-Phishing Working Group, www.apwg.com.
- Phishing Activity Trends, Report for the Month of November, 2007, Anti-Phishing Working Group (APWG), apwg.org
- Gartner, Media Relations, 2008 Press Releases, "Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks", (http://www.gartner.com/it/page.jsp?id=565125), 05-March-2008.
- Joris Evers, Staff Writer, "PayPal fixes phishing hole", CNET News.com,

(http://www.news.com/PayPal-fixes-phishing-hole/2100-7349_3-6084974.html) , Published: June 16, 2006 4:12 PM PDT.
- Sebastian Bauer, “Knorr.de SQL Injection and XSS Vulnerabilities”, (http://blog.gjl-network.net/blog/index.php?/archives/78-Knorr.de-SQL-Injection-and-XSS-Vulnerabilities.html) , 01/12/07.
- http://www.antiphishing.org/phishing_archive/Citibank_3-31-04.htm
- Ingrid Marson, “Firefox flaw raises phishing fears”, (http://www.news.com/Firefox-flaw-raises-phishing-fears/2100-1002_3-5517149.html), Published: January 7, 2005 11:06 AM PST
- Network Working Group, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999, (http://tools.ietf.org/html/rfc2616)
- “Microsoft Phishing Filter: A New Approach to Building Trust in E-Commerce Content”, anti-phishing white paper, Microsoft.com,2005